secorvo
security consulting

Secorvo Security News

Januar 2008

Editorial: Abgeschöpft

Skimming („Abschöpfen") heißt die neue Kampfansage an bargeldlose Zahlungsmittel, nachdem es zumindest in Deutschland schwieriger geworden ist, mit Phishing reich zu werden. Zwar ist das Abgreifen der PIN am Geldautomaten keine ganz frische Idee: Erste Betrugsfälle, bei denen mittels präparierter Tastatur (Pulver o.ä.) die PIN-Ziffern am Geldautomaten ausgespäht und anschließend die EC-Karte entwendet wurde, gab es schon vor über 15 Jahren.

Die Entwicklung kleinster digitaler Kameras und Kartenleser ermöglicht heute jedoch „Massenattacken" durch die Konstruktion täuschend echter Attrappen für Kartenleser und Tastatur. Dabei werden die Daten der eingeschobenen EC-Karte vom aufgesetzten Lesegerät kopiert und die PIN-Eingabe mit einem Tastaturaufsatz oder mittels winziger verborgener Video-Kameras aufgezeichnet. Anschließend übermittelt die Attrappe die Daten per Funk oder speichert sie auf einem Flash-Chip. Die damit geklonten EC-Karten funktionieren zwar nur im Ausland – dafür kann das Tageslimit meist mehrmals abgeschöpft werden, bevor das Konto gesperrt wird.

2007 wurden in Deutschland 10.400 Skimming-Fälle mit insgesamt 41.000 betrügerischen Abhebungen gezählt – fast doppelt so viele wie 2006. Einige der Täter ließen sich bei der Montage der Attrappen sogar fotografieren und filmen. Und es dürfte noch schlimmer kommen: Denn nicht nur 53.000 Geldautomaten sondern auch die rund 600.000 Point-of-Sales-Terminals sind ein attraktives Ziel – erste manipulierte Geräte, die PIN und Daten per SMS verschicken, wurden bereits entdeckt. Und die PIN-Zahlungen im EC-Cash-Verfahren steigen seit Jahren. Quelle des Übels ist die Speicherung der Kartendaten auf Magnetstreifen statt auf zugriffsgeschützten Chips, einer seit über 15 Jahren verfügbaren Technik. Bis zur Nachrüstung hilft manchmal das Abdecken der PIN-Eingabe mit der freien Hand. Vom Rütteln am Automaten hingegen wird abgeraten – ein Zerstören der Attrappe könnte den Zorn in der Nähe wartender Täter erregen.

Inhalt

secorvo
security consulting

Security News

Router ohne Hosen

Von Tomaz Bratusa wurde am 07.01.2008 eine Session-Riding-Schwachstelle in der Router-Serie Linksys WRT54GL veröffentlicht. Ist ein Benutzer per Browser auf dem Router angemeldet, kann die Firewall des Routers durch einfaches Klicken auf einen präparierten Link deaktiviert werden. Die Routereinstellungen werden gemäß den in der URL übergebenen Parametern ohne weitere Bestätigung verändert, wenn ein Browser-Cookie der authentifizierten Sitzung hinterlegt ist.

Da bei Heimarbeitsplätzen die Firewall des Routers oft die einzige Schutzbarriere zum Internet darstellt und nicht immer zusätzlich eine Personal Firewall eingesetzt wird, besteht eine direkte Gefährdung für die dem Router nachgelagerten Endsysteme. Daher wird dringend empfohlen, administrative Tätigkeiten am Router und Surfen – auch das Recherchieren von Routerkonfigurationen – nicht zeitgleich oder zumindest nicht mit demselben Browser durchzuführen.

Grundsätzlich ist es ohnehin empfehlenswert, die Standardeinstellungen des Routers (wie Kennworte und voreingestellte IP-Netzbereiche) vor Inbetriebnahme zu ändern.

Kompass IT-Sicherheitsstandards

Der in Zusammenarbeit zwischen dem NIA und dem Bitkom erarbeitete Kompass der IT-Sicherheitsstandards wurde am 03.12.2007 in einer neuen Version 3.0 vorgestellt. Der Kompass gibt eine aktuelle Übersicht und Bewertung aller verfügbaren nationalen und internationalen Standards mit Bezug zur IT-Sicherheit. Den Autoren ist es gelungen, eine knappe und sehr hilfreiche Handreichung zu erstellen, die sowohl für IT-Sicherheitsverantwortliche als auch für Geschäftsführer und IT-Führungskräfte ein Leitfaden bei der Planung und Umsetzung von IT-Sicherheitskonzepten sein kann.

Im Rahmen des Sicherheitsmanagements spielen qualifizierte Audits eine immer wichtigere Rolle, daher haben wir den Standard ISO 19011:2002 „Guidelines for quality and/or environmental management systems auditing" vermisst. Auch auf die aktuelle Weiterentwicklung der ISO Standards 27xxx wird nicht eingegangen: So fehlt der Ausblick auf die Standards zu Benchmarking (ISO 27004), Management von Informationssicherheits-Risiken (ISO 27005) und Disaster Recovery Services (ISO 27006). Dies trübt den ansonsten sehr positiven Gesamteindruck allerdings nur minimal.

OpenSource Grundschutztool

Die SerNet GmbH publizierte am 21.01.2008 das OpenSource Grundschutztool Verinice in der Version 0.6. Es unterstützt das Sicherheitsmanagement und die Durchführung von Audits auf der Basis von IT-Grundschutz und ist – im Unterschied zu den etablierten Grundschutztools – kostenfrei erhältlich, sowohl für Windows, als auch für Linux und MacOS. Alle Versionen des Tools sind als Download verfügbar.

Unsere ersten Testeindrücke waren sehr positiv. Das Werkzeug zeichnet sich durch eine intuitive Bedienbarkeit, ein erweiterbares Objektmodell und die Möglichkeit zur Anbindung an verschiedene Datenbanken aus.

Infra-Root

Am 11.01.2008 berichtete die Online-Ausgabe der britischen „Telegraph", dass es einem Jugendlichen gelungen sei, mittels einer TV-Fernbedienung Wiechen der U-Bahn in Lodz umzustellen und so mindestens eine Entgleisung zu verursachen. Die technischen Details bleiben in dem Bericht im Dunkeln – zweifellos aber war die fehlende gegenseitige Authentisierung der beteiligten Geräte wieder einmal (vgl. SSN 04/2007) Hauptursache für das Problem. Statt eines Challenge-Response-Verfahrens wird bei Infrarot-Steuerungen bestenfalls ein Authentisierungscode übermittelt, der grundsätzlich (mit mehr oder weniger hohem Aufwand) kopiert und erneut „eingespielt" werden kann. Bei einfachen Systemen werden moderne programmierbare Fernbedienungen sowie viele PDAs bzw. Mobiltelefone so im virtuellen Handumdrehen über ihre Infrarot-Schnittstelle zum Angriffswerkzeug.

Die meisten Automobilhersteller haben bei ihren Zentralverriegelungen inzwischen professionellere Lösungen implementiert, die von einer einfachen Fernbedienung nicht „erlernt" werden können. Man sollte also erwarten können, dass Systeme mit einem höheren Gefährdungspotential mit mindestens der gleichen Sorgfalt konzipiert werden. Dennoch hat es in der Vergangenheit weitere und ähnliche Vorfälle gegeben. Unsere Empfehlung für's neue Jahr: Hausaufgaben nachholen!

Mit Spammern Geld verdienen

Nicht immer enthalten Spam-E-Mails URLs, auf die man klicken soll, oder Bilder von beworbenen Produkten. Seit einiger Zeit werden reine Text-E-Mails verschickt, die den Kauf bestimmter Aktien bewerben – so genannter „Stock Spam".

Wer sich immer schon gefragt hat, wie und warum derartige Aktionen erfolgreich sein können, dem sei die 39-seitige Anklageschrift zu Alan Ralsky als Lektüre empfohlen: Ralsky gilt seit vielen Jahren als einer der internationalen Top-Spammer, konnte aber nie verhaftet werden. Am 03.01.2008 nun wurden er sowie zehn weitere Personen weltweit angeklagt. Ihnen wird vorgeworfen, über einen Zeitraum von mindestens 21 Monaten durch das Versenden von bis zu mehreren Millionen Spam-E-Mails pro Tag einen Gewinn von geschätzten 2,6 Millionen US-Dollar eingestrichen zu haben.

Dazu kauften sie zunächst gezielt die (niedrig-preisigen) Aktien chinesischer Unternehmen und bewarben diese anschließend via Spam. Etliche Käufer trieben dann den Wert der Aktien in die Höhe, so dass die Spammer ihre Aktienpakete teuer verkaufen konnten. Die gesamte „Aktion" umfasste die Manipulation von Aktienpaketen, Registrierung gefälschter Domains, Bestechung von E-Mail-Server-Administratoren sowie das Mieten von Botnetzen (vgl. SSN 05/2005).

15 Jahre und kein bisschen leise...

Kaum eine andere Security-Veranstaltung zieht seit so vielen Jahren so viele Sicherheitsexperten an: Der DFN Workshop „Sicherheit in vernetzten Systemen" findet in diesem Jahr schon zum 15. Mal statt. Wieder einmal verspricht das Programm, an dessen Erstellung Stefan Kelm als Mitglied des Programmkomitees mitgewirkt hat, sowie die schon legendäre Abendveranstaltung Highlights zu aktuellen Themen der IT-Sicherheit. Auch Secorvo ist – wie in jedem Jahr – an dem Workshop beteiligt: Dirk Fox wird über Realisierung, Grenzen und Risiken der 'Online-Durchsuchung' vortragen.

Kreditscoring im Fokus

Für viele Datenschützer ist der Einsatz von Scoring-Verfahren, mit denen Banken die Bonität ihrer Kunden analysieren, ein rotes Tuch. Denn dabei wird bei Privatkunden oft erheblich in der Persönlichkeitssphäre „gewühlt" – und die unterliegt dem Schutz des Bundesdatenschutzgesetzes (BDSG).

Zahlreiche Kreditinstitute nehmen es jedoch offenbar mit dem BDSG nicht so genau, wie eine am 23.01.2008 vom Bundesverband der Verbraucherzentralen vorgelegte Studie zur Kreditscoring-Praxis in Deutschland zeigt. In über 90% der Stichproben wurden Testpersonen nicht über den Scoring-Wert informiert, in 30% der Fälle wurde nicht einmal eine Einwilligung zur Schufa-Anfrage eingeholt. Schließlich wurden z.T. äußerst fragwürdige Angaben wie „Wohndauer", „Arbeitgeber", „berufliche Stellung" und „Umzugshäufigkeit" erhoben.

Hackers Challenge

Die US-amerikanische Firma Digital Armaments Inc. hat am 04.01.2008 eine Hacker Challenge gestartet, die jede bis zum 29.02.2008 eingereichte neue Schwachstelle mit funktionsfähigem Exploit-Code mit 20.000 US$ prämiert. Das Geschäftsmodell des 2003 gegründeten Unternehmens ist interessant: Es versucht, Hacker zur Zusammenarbeit zu gewinnen und schreibt seit April 2006 immer wieder thematische Hacker Challenges aus. Geld verdient das Unternehmen mit dem Verkauf exklusiver Reports über die eingereichten (und möglicherweise auch selbst gefundenen) Schwachstellen.

Genau so müsste es das organisierte Verbrechen wohl machen, um günstig an unveröffentlichte Exploits zu kommen. Oder BND, BKA und Verfassungsschutz – für die Online-Durchsuchung.

Sicherheitsstudie 2008

Seit vielen Jahren sind die Ergebnisse der IT-Sicherheitsstudie der Zeitschrift KES, die alle zwei Jahre erstellt wird, für viele Sicherheitsbeauftragte eine große Hilfe – denn „belastbare" Zahlen, mit denen sich eigene Risikoeinschätzungen und Investitionsentscheidungen stützen lassen, gibt es viel zu wenig.

Den pdf-Fragebogen für die Sicherheitsstudie 2008 gibt es online unter www.kes.info/studie2008. Die Auswertung erfolgt anonym. Alle Teilnehmer erhalten exklusiven Zugriff auf die tabellarische Auswertung sowie ein Präsent. Einsendeschluss für den ausgefüllten Fragebogen ist der 01.03.2008.

Secorvo News

Secorvo College aktuell

Im vergangenen Jahr hat sich die Zahl der TISP-Absolventen auf mehr als 200 verdoppelt – und die Nachfrage reißt nicht ab. Damit ist der TISP auf dem Weg zum führenden beruflichen Weiterbildungszertifikat im Gebiet IT-Sicherheit. Vom **25.–29.02.2008** bietet Secorvo College mit der fünftägigen T.I.S.P.-Schulung die nächste Gelegenheit, ein TISP-Zertifikat zu erwerben.

Anfang März (**11.–14.03.2008**) bietet das Seminar PKI - Grundlagen, Vertiefung, Realisierung genau das Wissen und die Erfahrung, die für die zielorientierte Entwicklung und den effizienten Betrieb einer PKI unabdingbar sind.

Das gesamte Seminarangebot 2008 sowie ein Online-Anmeldeformular finden Sie unter http://www.secorvo.de/college.

Veranstaltungshinweise

Auszug aus http://www.veranstaltungen-it-sicherheit.de

Februar 2008	
05.-06.02.	18. SmartCard Workshop (Fraunhofer, Darmstadt)
10.-13.02.	Fast Software Encryption Workshop (FSE 08) (IACR, Lausanne/CH)
13.-14.02.	15. DFN CERT & PCA Workshop - Sicherheit in vernetzten Systemen (DFN-CERT, Hamburg)
25.-29.02.	T.I.S.P.-Schulung (Secorvo College, Karlsruhe)
März 2008	
09.-12.03.	11. International Workshop on Practice and Theory in Public Key Cryptography (IACR, Barcelona/ES)
11.-14.03.	PKI - Grundlagen, Vertiefung, Realisierung (Secorvo College, Karlsruhe)
19.-21.03.	5. Theory of Cryptography Conference (TCC 2008) (IACR, New York/US)
April 2008	
01.-03.04.	Forensik - Verfahren, Tools, Praxiserfahrung (Secorvo College, Karlsruhe)
14.-17.04.	Eurocrypt 2008 (IACR, Istanbul/TR)
15.-18.04.	Information Security Management - von A(udit) bis Z(ertifizierung) (Secorvo College, Karlsruhe)
15.04.	First USENIX Workshop on Large-scale Exploits and Emergent Threats (Usenix, San Francisco/US)
22.-23.04.	Identity Management Symposium 2008 (Secorvo, Karlsruhe-Ettlingen)

Impressum

http://www.secorvo-security-news.de

ISSN 1613-4311

Redaktion: Dirk Fox, Stefan Gora, Kai Jendrian, Stefan Kelm, Jochen Schlichting

Herausgeber (V. i. S. d. P.): Dirk Fox
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses:
security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an
redaktion-security-news@secorvo.de

secorvo
security consulting

Secorvo Security News

Februar 2008

Editorial: Captcha

Informatiker kennen den nach seinem Erfinder Alan Turing (1912-1954) benannten Turing-Test, in dessen Verlauf ein Mensch in fünf Minuten entscheiden soll, welcher von zwei mit ihm über einen Computer verbundenen Gesprächspartnern eine Maschine und welcher ein Mensch ist. Bis heute hat es kein Computerprogramm geschafft, einen menschlichen Tester zu täuschen.

Diese Frage nach der Unterscheidbarkeit von „künstlicher" und „menschlicher" Intelligenz, die in den 80er Jahren die Informatik aufwühlte, ist heute hinter eine andere zurückgetreten: Kann ein *Computer* entscheiden, ob ein Computer mit ihm spricht? Dieser gewissermaßen „umgekehrte Turing-Test" entwickelt sich zur Schlüsselfrage zahlreicher Web-Angebote. Denn vielfach sind automatische „Gesprächspartner" unerwünscht, wie z. B. Antwort-Automaten bei Wissenstests, Trojaner beim Online-Banking oder Spam-Bots, die Suchmaschinen für die Recherche von E-Mail-Adressen einspannen und News-Weiterleitungen für Postings missbrauchen.

Als Fachbegriff für solche Tests hat sich das Akronym „CAPTCHA" durchgesetzt: *Completely Automated Public Turing test to tell Computers and Humans Apart*. Dabei wird dem Nutzer des Angebots eine Aufgabe gestellt, die möglichst nur ein Mensch lösen kann – meist das Herauslesen verfremdeter Ziffern und Buchstaben aus einer Grafik. In zahlreichen Anwendungen werden solche Bild-CAPTCHAs inzwischen als Sicherheitsmechanismus eingesetzt. Ein Problem dieser CAPTCHA-Mechanismen ist, dass für viele nach und nach automatische Lösungen entwickelt werden, und daher deren Komplexität ständig zunimmt. Je komplizierter aber das CAPTCHA, desto schwerer ist es auch für einen Menschen zu lösen.

Austricksen lassen sich CAPTCHAs aber noch viel einfacher: Präsentiert ein Online-Banking-Trojaner ein abgefangenes CAPTCHA auf einer vielbesuchten Erotik-Seite, erhält er die Lösung in Sekunden „frei Haus" – beantwortet von einem unwissentlichen Mittäter. Sicherheit ist eben mehr als die Summe guter Mechanismen.

Inhalt

secorvo
security consulting

Security News

TrueCrypt 5

Die freie Software TrueCrypt zur Verschlüsselung von Daten auf Festplatten ist am 05.02.2008 in der Version 5 erschienen. Highlight der Neuerungen ist die Möglichkeit, nun auch die komplette Festplatte inklusive Betriebssystem zu verschlüsseln. Weiter wurde erstmals eine Version für Mac OS X veröffentlicht, und Linux-Benutzer können sich endlich über eine grafische Oberfläche freuen. Zusätzlich gab es einige Detailänderungen bei den genutzten kryptografischen Verfahren.

Erste Tests bestätigen den guten Eindruck früherer Versionen der Software. Sowohl die Vollverschlüsselung als auch die Kompatibilität mit alten Versionen funktionierten problemlos. TrueCrypt ist eine gut gemachte, kostenlose Verschlüsselungssoftware. Neben vielen guten Eigenschaften lässt sie allerdings einige für den Einsatz in Enterprise-Umgebungen wichtige Funktionalitäten wie z. B. Mehrbenutzerfähigkeit und PKI-Anbindung vermissen.

Leitfaden Kritis

Am 24.01.2008 stellte Staatssekretär Dr. August Hanning vom Bundesministerium des Inneren den neuen Leitfaden „Schutz Kritischer Infrastrukturen - Risiko- und Krisenmanagement" vor. Das 87-seitige Dokument wendet sich primär an Behörden und Unternehmen mit Verantwortung im Bereich KRITIS. Der Leitfaden beschreibt die Phasen Vorplanung, Risikoanalyse, Vorbeugende Maßnahmen und Krisenmanagement und stellt einen umfangreichen Anhang mit Literatur, Gefahrenlisten, Checklisten und einer beispielhaften Risikoanalyse zur Verfügung. Auch für Unternehmen und Behörden, die nicht zu den primären Adressaten des Leitfadens zählen, enthält das Dokument interessante Ansätze für Risiko- und Krisenmanagement. Weitere gute Dokumente zum Thema bietet die Risk Management Series der amerikanischen Federal Emergency Management Agency (FEMA).

ITGK-Ergänzung 9

Seit dem 15.02.2008 ist die 9. Ergänzungslieferung der IT-Grundschutzkataloge online und zum Download auf den Seiten des Bundesamtes für Sicherheit in der Informationstechnik (BSI) verfügbar. Eine angepasste Version des Grundschutztools GSTOOL ist angekündigt.

Die Weiterentwicklung umfasst neue Bausteine, die sich u. a. mit Themen wie elektrotechnischer und IT-Verkabelung, Netzdruckern, Datenträgeraustausch und dem unscheinbaren, aber immer wichtigeren Thema „mobile Datenträger" beschäftigen. Zusätzlich sind neue Maßnahmen und Gefährdungen in die Kataloge eingearbeitet worden.

Auch sprachlich passt das BSI die Kataloge dem wachsenden Bedürfnis nach umfassender Informationssicherheit an. Sukzessive wird der etablierte Begriff „IT-Sicherheit" durch „Informationssicherheit" ersetzt – das ist ein sehr sinnvoller Schritt, geht es doch um den Schutz von Informationen unabhängig von der Form, in der sie vorliegen.

Metasploit 3.1

Am 28.01.2008 wurde Version 3.1 des Metasploit Project vorgestellt, dessen Ziel es ist, Penetrationstestern, Forschern und Exploit-Entwicklern aktuelle Informationen und Hilfsmittel zu Exploit-Techniken verfügbar zu machen. Die neue Version enthält Werkzeuge beispielsweise zur Sicherheitsüberprüfung von WLANs und des neuen Apple iPhone, wurde um weitere Funktionen ergänzt und bietet nun auch unter Windows eine vollständige grafische Oberfläche.

Ergonomie und Leistungsfähigkeit des Werkzeugs sind beachtlich. Wie so viele „dual use"-Produkte wird es in den falschen Händen allerdings zu einem mächtigen Angriffswerkzeug, mit dem sich erheblicher Schaden anrichten lässt.

Shmoocon 2008

Auf der diesjährigen Shmoocon (15.-17.02.2008) wurden eine ganze Reihe neuer Angriffstechniken vorgestellt. Besonders interessant waren das Entschlüsseln von GSM-Verbindungen mit vertretbaren Investitionskosten, potentielle Schwachstellen auf Citrix-Servern und das Einbringen von echten Exploits in virtuelle Welten wie „second live". Daneben wurden auch gesellschaftspolitische Themen wie die soziale Verantwortung der Hacker-Community diskutiert und Hilfsprojekte wie Hackers for Charity vorgestellt.

In seiner Keynote am 15.02.2008 stellte Alex Halderman unglaubliche Sicherheitsmängel amerikanischer Wahlcomputer vor. Stimmt der Dateiname, wird ein infiziertes Systemimage anstandslos geladen und kann sich über eine PCMCIA-Speicherkarte auf weitere Wahlcomputer verbreiten. Prüfsummen und kryptografische Schutzmechanismen sucht man vergeblich; der PCMCIA-Schacht kann nur mit einem Schloss physikalisch gesperrt werden – das bau- und „schlüsselidentisch" mit einem bei Jukeboxen und Geldspielgeräten eingesetzten ist. Nach dem holländisch-deutschen Wahlmaschinen-Debakel (siehe SSN 10/2006) ist nun vielleicht auf politische Einsicht zu hoffen – auch bei der Entwicklung und Prüfung von Wahlmaschinen

sollte man jemanden fragen, der etwas davon versteht. Die Vortragsunterlagen und Videos der gelungenen Veranstaltung können in Kürze von der Website geladen werden.

Protokollierung

Das Thema Protokollierung ist so etwas wie die Achillesferse der IT-Sicherheit: fast jedes System bietet Protokolldaten, die Auswertungstools sind meist primitiv, die Formate uneinheitlich – und nicht jede Protokollierung ist zulässig. Mit der am 17.01.2008 veröffentlichten „Studie über die Nutzung von Log- und Monitoringdaten im Rahmen der IT-Frühwarnung und für einen sicheren IT-Betrieb“ will das BSI Licht in den Logdatendschungel bringen – und hat dem Thema möglicherweise einen Bärendienst erwiesen.

Die 294 Seiten umfassende Fleißarbeit listet die Merkmale von Logdateien wichtiger Systeme und Anwendungen auf, ignoriert aber die rechtlichen Anforderungen praktisch vollständig. Die wenigen Andeutungen zu Anforderungen des Datenschutzrechts sind irreführend bis falsch und lassen diesbezügliche Unkenntnis der Autoren vermuten; Hinweise auf Mitbestimmungspflicht und die Unzulässigkeit der Speicherung von Verbindungsdaten nach Telekommunikationsgesetz fehlen ganz. Von einer Umsetzung der Empfehlungen der Studie ohne vorausgehende Betrachtung der rechtlichen Anforderungen wird daher dringend abgeraten.

OWASP Publikationen

Veröffentlichungen der OWASP-Initiative sind seit Kurzem über den digitalen Verlagsmarktplatz LULU in gedruckter Form oder als formatiertes PDF verfügbar. Die Prints sind preislich sehr attraktiv, die PDFs kostenlos und tragen hoffentlich dazu bei, die qualitativ sehr hochwertigen Informationen der OWASP weiter zu verbreiten.

Der neue Gola/Wronka

Peter Gola und Georg Wronka haben Ihr Standardwerk „Handbuch zum Arbeitnehmerdatenschutz“ erneut überarbeitet und am 28.11.2007 in einer aktualisierten 4. Auflage herausgebracht.

Leider konnten sich die Autoren nicht von ihrem Konzept trennen, das sich an Verarbeitungsphasen orientiert, wodurch die Erörterung praktisch zusammenhängender Themen häufig in unterschiedlichen Kapiteln erfolgt. Auch wenn der Praktiker einige brandaktuelle Themen vermisst (z. B. Forensische Untersuchungen) und andere sehr allgemein abgehandelt werden (z. B. Whistleblowing), so bietet das Werk doch nach wie vor einen guten Überblick und stellt insbesondere die Verschränkung mit Mitbestimmungsfragen umfassend dar.

Secorvo News

Secorvo College aktuell

Die CeBIT wird es wieder zeigen: PKIs leben – wenn auch oft versteckt als „Treibsatz“ z. B. hinter E-Mail-Verschlüsselungslösungen. Wer verstehen will, wie PKIs funktionieren, wie sie aufgebaut und in Anwendungen und Verzeichnisdienste integriert werden, dem sei das Seminar PKI – Grundlagen, Vertiefung, Realisierung vom **11.–14.03.2008** ans Herz gelegt. Das Seminar umfasst praktische Übungen.

Der „Klassiker“ IT-Sicherheit heute wird wegen der hohen Nachfrage als Zusatztermin vom **27.–30.05.2008** stattfinden. Nach einer grundlegenden Überarbeitung und Aktualisierung deckt die Agenda jetzt in vier Tagen die wichtigsten aktuellen Themen der IT-Sicherheit ab. Eine Einführung in das Information Security Management von A(udit) bis Z(ertifizierung) mit Umsetzungsworkshop bietet Secorvo College vom **15.–18.04.2008**.

Detaillierte Programme, vollständige Jahresübersicht und Online-Anmeldung unter http://www.secorvo.de/college

Identity Management Symposium

In vielen Unternehmen existieren historisch bedingt zwei „Identitäts-Management“-Systeme unverbunden nebeneinander: Der Betriebsausweis, meist im Verantwortungsbereich der Corporate Security, und die Benutzerauthentifikation mit Rechnerzugang, in der Regel in der Zuständigkeit der IT-Security. Dabei kommt es zu Doppelarbeit, denn für beide Bereiche ist das Management eines „Berechtigungs-Lebenszyklus“ erforderlich.

Mit der Verbreitung elektronischer Zugangssysteme und Authentifikationslösungen, die Passworte durch Token ersetzen, rücken beide Systeme zusammen: Idealerweise sollten alle an die Identität eines Mitarbeiters gekoppelten Dienste über eine Karte möglich sein. Erste Unternehmen haben inzwischen ihre Identity Management-Systeme zusammengeführt. Die Komplexität dieser Projekte lag dabei sowohl in der Technik als auch in zahlreichen zu bewältigenden praktischen „Fallstricken“.

Gemeinsam mit der vps GmbH will Secorvo mit dem „Identity Management Symposium“ am **22.–23.04.2008** einen intensiven Erfahrungsaustausch mit und zwischen Unternehmen und Behörden initiieren, die ein solches integriertes „Identity Management“ vorbereiten oder bereits eingeführt haben (Programm, Online-Anmeldung).

Veranstaltungshinweise

Auszug aus http://www.veranstaltungen-it-sicherheit.de

März 2008	
09.-12.03.	11. International Workshop on Practice and Theory in Public Key Cryptography (IACR, Barcelona/ES)
11.-14.03.	PKI – Grundlagen, Vertiefung, Realisierung (Secorvo College, Karlsruhe)
19.-21.03.	5. Theory of Cryptography Conference (TCC 2008) (IACR, New York/US)
April 2008	
02.-04.04.	Sicherheit 2008 (GI, Saarbrücken)
14.-17.04.	Eurocrypt 2008 (IACR, Istanbul/TR)
15.-18.04.	Information Security Management - von A(udit) bis Z(ertifizierung) (Secorvo College, Karlsruhe)
15.04.	First USENIX Workshop on Large-scale Exploits and Emergent Threats (Usenix, San Francisco/US)
22.-23.04.	Identity Management Symposium 2008 (Secorvo, Karlsruhe-Ettlingen)
Mai 2008	
06.-07.05.	9. Datenschutzkongress 2008 (Euroforum, Berlin)
06.-08.05.	IT-Sicherheitsaudits in der Praxis (Secorvo College, Karlsruhe)
26.-29.05.	IT Sicherheitsforum 2008 (GAI Netconsult, Frankfurt)
27.-30.05.	IT-Sicherheit heute (Secorvo College, Karlsruhe)
Juni 2008	
02.-06.06.	T.I.S.P.-Schulung (Secorvo College, Karlsruhe)

Impressum

http://www.secorvo-security-news.de

ISSN 1613-4311

Redaktion: Dirk Fox, Stefan Gora, Kai Jendrian, Stefan Kelm, Karin Schuler

Herausgeber (V. i. S. d. P.): Dirk Fox
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses:
security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an
redaktion-security-news@secorvo.de

secorvo
security consulting

Secorvo Security News

März 2008

Editorial: Ach wie gut!

Heute back' ich, morgen brau' ich,
übermorgen hol' ich der Königin ihr Kind;
ach, wie gut dass niemand weiß,
dass ich Rumpelstilzchen heiß!

Das war es also. Dieses Märchen unserer Kindheit erklärt unser gespaltenes Verhältnis zum Datenschutz. Tief verinnerlicht haben wir, dass nur derjenige seinen richtigen Namen verheimlicht, der Böses im Schilde führt – wird er erkannt, reißt er sich selbst in Stücke. Und so glauben wir im Umkehrschluss, dass der Unbescholtene nichts zu verbergen habe. Streift man durch „soziale Netzwerke" wie myspace, facebook, Xing oder SchülerVZ, so drängt sich der Eindruck auf, als wollten Millionen aus dieser tief verankerten Überzeugung ihre Unbescholtenheit durch exzessives Nichtverbergen unter Beweis stellen.

Wehe aber, wenn die Erkenntnis dämmert, dass es vielleicht nicht immer gut ist, Dritten umfangreiche persönliche Informationen zur Verfügung zu stellen. So geschehen, als facebook ab 07.11.2007 zur Nutzung des verkaufsfördernden „me too"-Effekts die aktuellen Online-Einkäufe der registrierten Benutzer an deren Freundeslisten schickte. Aber auch unwissentlich geben viele Nutzer persönliche Informationen im Internet preis – so weiß beispielsweise nicht jeder, dass die private Wunschliste beim Online-Buchhändler Amazon von jedermann eingesehen werden kann, wenn die Voreinstellung nicht geändert wurde. Daher lohnt es, gelegentlich bei einer Personensuchmaschine wie Yasni das eigene „Bild im Netz" zu überprüfen.

Zugleich nimmt die Überwachung im Windschatten der Terrordrohung zu – ungeachtet der jüngsten Urteile des BVerfG zu Online-Durchsuchung und Vorratsdatenspeicherung, die dem behördlichen Zugriff auf persönliche Daten hohe Hürden auferlegen. Dabei gibt die älteste Demokratie Europas den Schritt vor: Nach der flächendeckenden Installation von Videokameras in britischen Großstädten soll zukünftig eine Bilddatenbank die automatische Identifikation Verdächtiger erlauben. Ein 18-monatiges Pilotprojekt mit 750.000 Fotos verlief offenbar vielversprechend. Ob es hilft, den Namen des Ideengebers herauszufinden – damit er sich selbst in Stücke reißt?

Inhalt

secorvo
security consulting

Security News

Mifare-Cloning

Auf dem Jahreskongress des Chaos Computer Clubs stellten Karsten Nohl und Henryk Plötz am 28.12.2007 einen Angriff auf das Authentifikationsverfahren kontaktloser Mifare-Chipkarten vor. Dem vom Hersteller geheimgehaltenen, etwa 15 Jahre alten "CRYPTO1"-Algorithmus waren sie mit einer Mikroskop-Analyse des Chip auf die Spur gekommen, um dann nach kryptographischen Schwächen (zu kleiner Zufallswert, lineares Schieberegister) darin zu suchen. Zu dieser Krypto-Schwachstelle gibt es nun den passenden „Mifare-Cloner“: Am 12.03. 2008 haben Forscher der Radboud Universiteit Nijmegen ein Video in YouTube veröffentlicht, auf dem sie zeigen, wie sie mit minimalem Aufwand Mifare-basierte Zugangskarten duplizieren.

Von der Attacke betroffen sind Tausende von Anwendungen mit einer Milliarde ausgegebenen Karten, vom Betriebsausweis über die Kantinenkarte bis zum bargeldlosen Bezahlsystem im öffentlichen Nahverkehr, sofern sie Mifare-Chips des Typs MF1 IC S50 oder S70 verwenden. Fein raus ist, wer seine Anwendung bereits auf den neueren Mifare DESFire (MF3 IC D40) migriert hat – statt einer etwas ältlichen Stromchiffre verwendet er bei der Authentifikation wahlweise DES oder TripleDES.

Fingerwischerei

In einem am 12.03.2008 online veröffentlichten Beitrag aus c't 05/08 beschreibt Daniel Bachfeld eine simple Methode, wie auf zahlreiche USB-Sticks unter Umgehung des Fingerprint-Schutz zugegriffen werden kann. Verwendet der Stick den Controller USBest UT176 oder UT 169 von Afa Technology, so erfolgt zwar die Fingerprint-Prüfung auf dem Chip – das Freigabe-Kommando für die „geschützte“ Partition sendet jedoch die Systemsoftware vom PC. Mit dem Open-Source-Tool PLscsi gelingt der Zugriff ohne Fingerkuppen-Imitat in nur drei Schritten.

Das Beispiel zeigt (leider) wieder einmal, dass es meist wenig hilft, einen Sicherheitsmechanismus nachträglich an eine bestehende Lösung „anzuflanschen“ – ist er nicht geeignet im System verankert, lässt sich das Verfahren an der Nahtstelle oft allzu leicht wieder auftrennen.

Einsatz von WAFs

Das OWASP German Chapter veröffentlichte am 18.03.2008 den deutschsprachigen Guide „Best Practices: Einsatz von Web Appliction Firewalls“. Das lesenswerte 25-seitige Dokument wendet sich an technische Entscheider im Bereich der Sicherheit von Web-Applikationen. Nach einer Einordnung von Web Application Firewalls (WAF) wird deren Haupteinsatzzweck erläutert – die nachträgliche Absicherung des externen Verhaltens von produktiven Web-Anwendungen, mit vertretbarem Aufwand und ohne Änderung der Applikation.

Die Betrachtung der Schutzmechanismen fokussiert auf den Schutz gegen die OWASP Top 10 (siehe SSN 06/2007). Abschließend werden Kriterien zur Einsatz-Entscheidung, Checklisten und Rollenmodelle für die Einführung sowie Best Practices für den Betrieb vorgestellt. Positiv fällt auf, dass in dem Dokument in allen Phasen Wert auf die Berücksichtigung von Aufwandsschätzungen gelegt wird.

Citrix-Ausbruch

Nicht nur bei einer Betriebssystemvirtualisierung sondern auch bei der Desktopvirtualisierung ist der Ausbruch aus einem beschränkten Kontext ein Risiko. So deckte Stefan Gora am 07.03.2008 auf, dass in Citrix-Umgebungen über den Microsoft-Taschenrechner auf weitere Applikationen zugegriffen werden kann, für die keine Berechtigung besteht. Denn unter Windows 2003 Server werden die Lizenzbedingungen des Taschenrechners mit dem Editor angezeigt, der über die Funktion „Datei öffnen“ das Starten weiterer Anwendungen ermöglicht.

Die Sicherheitslücke ist ein schönes Beispiel dafür, dass Hintertüren in komplexen Umgebungen manchmal ganz harmlos daherkommen. Zwar erlaubt der Taschenrechner unter den aktuelleren Microsoft-Server-Versionen diesen „Ausbruch“ nicht; dennoch empfehlen wir die Nutzung verschiedener Terminal-Server-Plattformen für Benutzergruppen mit unterschiedlichen Berechtigungen.

Rechenfehlerangriff

Zwei japanische Wissenschaftler veröffentlichten am 27.12.2007 einen Angriff auf den Advanced Encryption Standard (AES), der unter bestimmten Voraussetzungen 88 Bit eines 128-Bit-AES-Schlüssels rekonstruiert. Sie verwendeten dazu die auf den ersten Blick befremdlich anmutende Methode der „Differentiellen Fehleranalyse“ (DFA). In diesem speziellen Fall muss dazu ein bekannter Klartext mehrfach mit demselben Schlüssel verschlüsselt werden: Einmal ungestört, ein anderes Mal mit einem gezielt induzierten Fehler. Dabei muss der Angreifer erreichen, dass bei der neunten von zehn Runden eine bestimmte 32-Bit-Variable einen fehlerhaften Wert annimmt.

In der Praxis dürfte ein derartiger Angriff bei den meisten Anwendungen des AES nur äußerst schwer erfolgreich durchzuführen sein. Wer dennoch auf

Nummer sicher gehen will und die vierzigprozentige Leistungseinbuße nicht scheut, sollte den AES mit der maximalen 256 Bit Schlüssellänge verwenden – mit weiteren 128 Schlüsselbits und vier zusätzlichen Runden.

VMware-Hacks

Die am 25.02.2008 von Coresecurity veröffentlichte und vom Hersteller bestätigte Schwachstelle in VMware-Workstation und dem VMware-Player sollte nicht unterschätzt werden: Durch den Bug im Mechanismus der „Shared Folder" ist es möglich, von Wirtsbetriebssystemen aus auf das Hostsystem – und damit auf weitere Wirtssysteme – zuzugreifen. Die Abschottung der Systeme kann so vollständig ausgehebelt werden.

Unverständlich ist, dass bisher seitens VMware nur ein primitiver Workaround für die schon am 16.10. 2007 an den Hersteller gemeldete Schwachstelle vorliegt: die Empfehlung, „Shared Folder" zu deaktivieren.

Druckfrischer Entwurf

Auf den Webseiten des Bundesamt für Sicherheit in der Informationstechnik (BSI) steht der druckfrische Entwurf des „BSI Standards 100-4: Notfall-Management" in der Version 0.7 vom 19.03.2008 zum Download bereit. Die Veröffentlichung dieses schon lange erwarteten BSI-Standards zum Thema Business Continuity (BCM) und Notfall-Management verzögerte sich durch die Abstimmung mit den britischen Standards BS 25999-1:2006 und BS 25999-2:2007.

Das BSI bittet um kritische Prüfung und Kommentierung des aktuellen 82-seitigen Entwurfs bis Ende April 2008.

Krypto-Historie

Auf der Tagung „Día Internacional de la Seguridad de la Información" (DISI) gab Martin E. Hellman am 03.12.2007 an der Universidad Politécnica de Madrid einen spannenden Einblick in die Geburtsstunden der modernen Kryptographie („A Fool's Errand"). Sowohl seine Vortragsfolien als auch ein Video der Keynote sind inzwischen online verfügbar – die Dokumentation einer der Sternstunden der IT-Sicherheit.

Überraschend sein wenig technischer Ausblick: „What is the most important unsolved problem in cryptography? Lack of user awareness."

Secorvo News

Secorvo College aktuell

Eine Einführung in das Information Security Management von A(udit) bis Z(ertifizierung) inklusive Umsetzungsworkshop bietet Secorvo College vom **15.–18.04.2008.** Ein guter Einstieg für alle, die ihr Sicherheitsmanagement auf Standard-Konformität „abklopfen" möchten.

Das tatsächlich erreichte Sicherheitsniveau lässt sich auch durch ein Audit prüfen. Dazu bietet das Seminar IT-Sicherheitsaudits in der Praxis am **06.–08.05.2008** zahlreiche Hilfestellungen.

Am **27.–30.05.2008** wird der Klassiker IT-Sicherheit heute wieder aufgelegt – und deckt nach einer gründlichen Überarbeitung und Aktualisierung in vier Tagen die wichtigsten aktuellen Themen der IT-Sicherheit ab.

Und im Juni bietet sich Ihnen die nächste Gelegenheit, Ihre Fachkunde zu zertifizieren: auf dem T.I.S.P.-Seminar am **02.–06.06.2008**, mit anschließender Prüfung (Achtung: frühzeitige Anmeldung empfohlen).

Detaillierte Programme, vollständige Jahresübersicht und Online-Anmeldung unter http://www.secorvo.de/college

Aktualisierte White Paper

Eine aktualisierte Fassung des Secorvo White Papers „Das Policy-Rahmenwerk einer PKI" (Petra Barzin, Stefan Kelm) ist seit dem 27.03.2008 verfügbar.

Ebenfalls aktualisiert wurde die Forensik-Checkliste von Stefan Kelm (Version 1.2 vom 05.03.2008).

Identity Management Symposium

Gemeinsam mit der vps ID Systeme GmbH veranstaltet Secorvo am **22.–23.04.2008** das erste „Identity Management Symposium" in Ettlingen (bei Karlsruhe). Im Stil der bewährten Secorvo-Symposien wird es einen intensiven Erfahrungsaustausch mit und zwischen Unternehmen und Behörden bieten, die ein integriertes Identity Management vorbereiten oder bereits eingeführt haben. Unter anderem werden die Lösungen von BASF, BMW, ESG, Evonik, Fraunhofer und Swisscom vorgestellt (vollständiges Programm und Online-Anmeldung).

ITSF 2008

Das von GAI Netconsult und der ComConsult Akademie veranstaltete IT-Sicherheits-Forum 2008 findet in diesem Jahr vom 26.-29.05.2008 in Frankfurt statt. Auch diesmal wirkt Secorvo am Programm der etablierten Veranstaltung mit einem Tutorium zu „Security Awareness" und einer Keynote mit. Die Frühbucherphase endet am 31.03.2008.

Veranstaltungshinweise

Auszug aus http://www.veranstaltungen-it-sicherheit.de

April 2008	
02.-04.04.	Sicherheit 2008 (GI, Saarbrücken)
14.-17.04.	Eurocrypt 2008 (IACR, Istanbul/TR)
15.-18.04.	Information Security Management - von A(udit) bis Z(ertifizierung) (Secorvo College)
15.04.	First USENIX Workshop on Large-scale Exploits and Emergent Threats (Usenix, San Francisco/US)
22.-23.04.	1. Identity Management Symposium 2008 (Secorvo & vps, Karlsruhe-Ettlingen)
Mai 2008	
06.-07.05.	9. Datenschutzkongress 2008 (Euroforum, Berlin)
06.-08.05.	IT-Sicherheitsaudits in der Praxis (Secorvo College)
26.-29.05.	IT Sicherheitsforum 2008 (GAI Netconsult, Frankfurt)
27.-30.05.	IT-Sicherheit heute (Secorvo College)
Juni 2008	
02.-06.06.	T.I.S.P.-Schulung (Secorvo College)
09.-10.06.	DuD 2008 (Computas, Berlin)
17.-18.06.	6. Security Awareness Symposium (Secorvo, Karlsruhe-Ettlingen)
24.-25.06.	D-A-CH Security 2008 (GI/OCG/Bitkom/TTT, Berlin)
24.-26.06.	Sichere Softwareentwicklung (Secorvo College)
Juli 2008	
01.-03.07.	Forensik (Secorvo College)

Impressum

http://www.secorvo-security-news.de

ISSN 1613-4311

Redaktion: Dirk Fox, Stefan Gora, Kai Jendrian, Stefan Kelm, Hans-Joachim Knobloch

Herausgeber (V. i. S. d. P.): Dirk Fox
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses:
security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an
redaktion-security-news@secorvo.de

secorvo
security consulting

Secorvo Security News

April 2008

Editorial: „(T)Räumst du noch oder identifizierst du schon?“

Kontaktlose Chipkarten haben sich inzwischen auch in mittelständischen Unternehmen als Betriebsausweis durchgesetzt. Sie dienen als bargeldloses Zahlungsmittel im Betriebsrestaurant, regeln den Gebäudezugang und vereinfachen die Zeiterfassung. Von einer ähnlichen Infrastruktur träumt auch die IT: Gesteuert durch aktuelle HR-Prozesse (Eintritt, Austritt, interner Wechsel etc.) ließen sich Zugriffsrechte für zentrale Systeme und kryptographische Schlüssel (VPN-Einwahl, E-Mail- und Festplattenverschlüsselung) automatisch vergeben und wieder entziehen – abhängig von Aufgabe und Stellenbeschreibung, mit striktem Freigabeprozess nach dem Need-to-Know-Prinzip. Schließlich kann der Ausweis als Single-Sign-On-Token leidige Mehrfach-Logins ablösen.

Der Sicherheitsgewinn wäre erheblich – keine „vagabundierenden“ Accounts mehr, Schluss mit notierten, weitergegebenen oder trivialen Passworten, Ende der „Rechteakkumulation“ bei Mitarbeitern, die häufig den Zuständigkeitsbereich wechseln. Administrationsprozesse würden einfach, Hotline-Anrufe zur Passwortrücksetzung entfallen. Die subjektive Wahrnehmung von Sicherheitsmechanismen als Arbeitsbehinderung wäre endlich Geschichte.

Technisch ist dies keine Zauberei mehr. In der Praxis sind zuvor jedoch ein paar Aufräumarbeiten zu erledigen, die schon in mittelgroßen Unternehmen wie die Reinigung des Augiasstalls anmuten: So müssen Rechte in Rollen verdichtet, Freigabeprozesse etabliert und HR-Daten konsolidiert werden. Die Bewältigung dieser Herausforderungen, die ohne höchsten Management-Support nicht gelingen kann, lohnt jedoch – das zeigten die Vorträge und Diskussionen auf dem ersten „Identity Management Symposium“ in Ettlingen: Wer Ordnung schafft, gewinnt – Geld, Überblick und Sicherheit.

Wer beim Schachspiel nicht einmal die Figuren in Ordnung zu stellen weiß,
der wird es schlecht zu spielen verstehen; und wer nicht Schach bieten kann,
der wird auch nie schachmatt setzen können." - *Theresa von Ávila*

Inhalt

secorvo
security consulting

Security News

Online-Durchsuchung in der EU

Am 09.04.2008 hat die 42köpfige interministerielle Arbeitsgruppe „Online-Durchsuchung“ des österreichischen BMJ/BMI ihren Schlussbericht zur Online-Durchsuchung vorgelegt. In dem knapp 100seitigen Dokument kommen die Autoren zu dem Schluss, „dass die geheime Überwachung von privaten Rechnern ein besonders schwer wiegender Eingriff ist“, der unter Gesetzesvorbehalt stehe – und für den es derzeit in Österreich keine Rechtsgrundlage gibt. Der öffentlich gewordene Einsatz einer „Remote Forensik“-Software vom Herbst 2007, bei dem in kurzen Abständen Screenshots eines überwachten Systems an die Strafverfolgungsbehörden gesandt worden waren, wird in einem rechtlichen „Graubereich“ angesiedelt. Lesenswert ist die vergleichende aktuelle Übersicht der Regulierung und des Standes der politischen Diskussion zur Online-Durchsuchung in den Mitgliedsstaaten der EU.

Registry Ripper

Immer öfter erfordert die forensische Analyse von Windows-Rechnern eine zeitaufwändige Untersuchung der Registry (NTUSER.DAT, etc.), da das Betriebssystem dort eine Vielzahl von Aktionen protokolliert, beispielsweise die zuletzt geöffneten Dateien und eine Liste gestarteter Anwendungen, geöffneter Netzwerk-Ports und besuchter Webseiten.

Obwohl nicht nur frei verfügbare Registry-Viewer, sondern auch (fast) alle Forensik-Toolkits detaillierte Auswertungsmöglichkeiten für die Registry bieten, artet die Analyse in der Praxis oft in "Herumgestochere" mit manueller Auswertung bestimmter Registry-Schlüssel aus. Dagegen hilft das am 09.04.2008 veröffentlichte Tool RegRipper (v2.01A vom 20.04.2008): Es wertet die ca. 50 wichtigsten in der Registry vorhandenen Schlüssel aus, kodiert dabei Binärwerte in eine lesbare Form, extrahiert vorhandene Zeitstempel und speichert das Ergebnis in einer effizient weiter zu bearbeitenden Textdatei. Die zu untersuchenden Teilbäume der Registry werden über programmierbare, leicht anpassbare Plugins gesteuert. Das Tool erfordert dabei keine Installation und verfügt neben einer Kommandozeile auch über eine graphische Benutzeroberfläche; außerdem wird der Perl-Quellcode mitgeliefert. Bereits diese vom Autor "Basic edition" genannte Version sollte in keiner forensischen Tool-Sammlung fehlen – der Autor hat bereits angekündigt, an einer stark erweiterten Version zu arbeiten.

Datenschutz international

Im Auftrag der Europäischen Kommission erstellten wik-Consult und RAND Europe eine Gegenüberstellung der Datenschutz-Regulierung in Europa, den USA, Japan, Südkorea, Malaysia und Indien. Die vom 20.07.2007 datierende Endfassung der Studie wurde am 29.02.2008 von der EU-Kommission publiziert.

Bewertet wurden insbesondere der Rechtsschutz, der Grad an Selbstregulierung, die Effektivität, die Rechtsdurchsetzung und das Spannungsverhältnis zu Sicherheitsgesetzen. Die 230seitige Studie basiert auf rund 40 Interviews mit Experten aus unterschiedlichen gesellschaftlichen Bereichen (Unternehmen, Regierungen, Datenschutzbehörden, Juristen und Verbraucherschutzverbänden) und bietet einen guten Überblick der Datenschutz-Gesetzgebung der jeweiligen Länder sowie des dahinter stehenden Regulierungskonzepts.

Voreingestellte WPA-Keys

Am 14.04.2008 veröffentlichte Kevin Devine unter gnucitizen.org den von Britisch Telekom für den WLAN-Router Thompson Speedtouch verwendeten Algorithmus zur Erzeugung der voreingestellten WEP- und WPA-Schlüssel: ein einfacher SHA-1-Hash der hexadezimal dargestellten Seriennummer. Für die WEP-Keys von Netopia-Routern entdeckte und publizierte er das Verfahren schon am 29.09.2007: ein SHA-1-Hash der Seriennummer mit angehängter Textzeile aus „Third Stone From The Sun" von Jimi Hendrix liefert den Schlüssel. Von „James67“ wurde kürzlich auch der Erzeugungsalgorithmus der Default-Keys des Routers Netgear V1 DG834GT gefunden – am 21.02.2008 riet Sky Broadband zum sofortigen Wechsel des WiFi-Keys.

Ursache des Übels, von dem viele weitere WLAN-Router unterschiedlicher Hersteller und vielleicht auch deutsche Provider betroffen sein dürften, sind das fehlende Verständnis für die Wichtigkeit einer *zufälligen* Schlüssel-Wahl – und die Bequemlichkeit der meisten Nutzer, die den voreingestellten Schlüssel nicht wechseln. Dazu raten wir dringend – denn auch wenn der Erzeugungsalgorithmus nicht veröffentlicht ist oder sogar Zufallswerte erzeugt, kennen Hersteller oder Online-Provider den Schlüssel. Damit ist die Kommunikation – auch ohne „Bundestrojaner“ – potentiell Dritten zugänglich.

All Your iFrames Point to Us

Seit mehr als 1,5 Jahren untersucht Google Webseiten auf Malware, die automatisch beim Aufruf der Seite installiert wird. Dabei wurden über drei Millionen unterschiedliche, mit Malware verseuchte URLs auf mehr als 180.000 Webseiten gefunden, wie Niels Provos am 11.02.2008 berichtete. Der

Anteil infizierter Seiten hat sich dabei von April 2007 bis Januar 2008 auf ca. 1,3% verdreifacht; mehr als die Hälfte (über 60%) der Seiten stammt aus China.

Details der zusammen mit der Johns Hopkins University durchgeführten Untersuchung finden sich in einem von Niels Provos veröffentlichten, 22seitigen Technical Report. Besonders lesenswert ist das vom 07.04.2007 datierende (9seitige) Grundlagenpapier The Ghost in the Browser, in dem Provos mit seinen Koautoren an Javascript-Beispielen erläutert, wie Webseiten-Malware arbeitet – und entdeckt werden kann.

Wurm inklusive

Am 03.04.2008 wurde bekannt, dass „USB Floppy Drive Keys" der Firma HP, eine optionale Ergänzung für ca. 40 Modellvarianten der Proliant-Serie, mit zwei Würmern verseucht ausgeliefert worden waren. Bei den Würmern handelte es sich um Fakerecy und SillyFDC, die sich auf alle angeschlossen lokalen und vernetzen Laufwerken verbreiten. Sie waren erstmals Mitte Januar bzw. Ende Februar 2008 aufgetaucht. Über eine Schadfunktion verfügen beide Würmer glücklicherweise nicht, und aktuelle Virenscanner erkennen und beseitigen sie vollständig. Dennoch zeigt der Vorfall, was bei mangelhafter Qualitätssicherung in der Hardwareproduktion drohen kann – erst im September 2007 waren einzelne iPods mit dem Virus RavMon.Exe ausgeliefert worden. Der nächste Wurm kommt bestimmt. Hoffentlich einer, den der Virenscanner erkennt.

Finger-Logger

Nicht erst seit der Ausspähung und Publikation des Fingerabdrucks des Bundesinnenministers durch den Chaos Computer Club Ende März 2008 ist bekannt, dass biometrische Merkmale gefälscht werden können – siehe z.B. den von Matsumoto auf der Eurocrypt 2002 publizierten Beitrag „Gummi Fingers" (SSN 1/2002).

Auf der Blackhat Europe wurde am 04.04.2008 eine exemplarische Analyse für einen biometrischen Scanner nebst Infrastruktur (Türzugang) vorgestellt. Durch eine Man-in-the-Middle-Attacke wurden die Daten aus dem Kommunikationsstrom erfolgreich rekonstruiert, da sie unverschlüsselt übertragen wurden. Die gewonnen Datenschablonen (Position, Datensatz und Fingerfolge) und Bilddaten wurden nach einem bekannten Verfahren zu einem funktionsfähigen Fingerabdruck weiterverarbeitet. Nach Keyloggern, Mini-Videokameras und Skimming-Attrappen müssen wir uns möglicherweise bald auch nach Biodaten-Loggern umschauen.

Vorratsdatenspeicherung

Am 11.3.2008 entschied das Bundesverfassungsgericht im Eilverfahren über die Verfassungsbeschwerde von über 34.000 Beschwerdeführern gegen die mit der Änderung von TKG und StPO eingeführte Vorratsdatenspeicherung. Zwar setzte es nicht – wie von den Beschwerdeführern erhofft – die Speicherung selbst außer Vollzug, sondern verbot befristet bis zum 11.09.2008 lediglich die Datenherausgabe an die Strafverfolgungsbehörden.

Das Gericht verpflichtete die Bundesregierung zur Abfassung eines Berichts über die praktischen Auswirkungen der Sperrung. Damit traf das BVerfG keine Vorentscheidung über die Speicherung, sondern vermied zunächst nur etwaige negative Folgen für die Betroffenen im Falle einer späteren Feststellung der Verfassungswidrigkeit der Regelungen.

Secorvo News

Secorvo College aktuell

Einen tiefen Einblick in IT-Sicherheitsaudits in der Praxis bietet Secorvo College am **06.–08.05.2008**. Am **27.–30.05.2008** findet wieder der „aktuelle Klassiker" statt – IT-Sicherheit heute. Nur noch wenige Plätze gibt es für das TISP-Seminar, das Secorvo College am **02.–06.06.2008** mit anschließender Prüfung durchführen wird. Programm und Online-Anmeldung unter http://www.secorvo.de/college.

DuD 2008 – die zehnte

Für die diesjährige 10. Fachkonferenz „DuD 2008" am **09.–10.06.2008** in Berlin unter der fachlichen Leitung der Herausgeber der Zeitschrift „Datenschutz und Datensicherheit" konnten wieder spannende Vorträge gewonnen werden. Darunter finden sich die Themen Whistleblowing, Internet-Bewertungen von Lehrkräften, IT-Virtualisierung, das Audit-Gesetz, Computerkriminalität und das „Web 2.0". Burkhard Hirsch, Bundesinnenminister a.D., wird zu den gesellschaftlichen Folgen staatlicher Überwachung Stellung beziehen, Prof. Christof Paar seine Attacke auf Wegfahrsperren vorstellen und Jan Krissler vom Chaos Computer Club über die jüngsten Angriffe auf Biometrie-Systeme berichten.

Pimp your web

Am **29.05.2008** widmet sich die Karlsruher IT-Sicherheitsinitiative (KA-IT-Si) dem Schutz von Web-Applikationen. Maximilian Dermann von Lufthansa Technik wird vorstellen, wie diese sich insbesondere vor DoS-Angriffen schützen lassen.

Veranstaltungshinweise

Auszug aus http://www.veranstaltungen-it-sicherheit.de

Mai 2008	
06.-07.05.	9. Datenschutzkongress 2008 (Euroforum, Berlin)
06.-08.05.	IT-Sicherheitsaudits in der Praxis (Secorvo College)
26.-29.05.	IT Sicherheitsforum 2008 (GAI Netconsult, Frankfurt)
27.-30.05.	IT-Sicherheit heute (Secorvo College)
29.05.	Pimp your web (KA-IT-Si, Karlsruhe)
Juni 2008	
02.-06.06.	T.I.S.P.-Schulung (Secorvo College)
09.-10.06.	DuD 2008 (Computas, Berlin)
17.-18.06.	6. Security Awareness Symposium (Secorvo, Karlsruhe-Ettlingen)
24.-25.06.	D-A-CH Security 2008 (GI/OCG/Bitkom/TTT, Berlin)
24.-26.06.	Sichere Softwareentwicklung (Secorvo College)
Juli 2008	
01.-03.07.	Forensik (Secorvo College)

Fundsache

Das freie E-Book „Security Concepts“ von Travis Howard, veröffentlicht am 12.04.2008, hat zwar mit 120 Seiten noch Projektcharakter, aber die übersichtliche Struktur, die Inhalte und insbesondere die starke Verlinkung zu externen Quellen machen das Werk zu einem lesenswerten Reiseführer für Sicherheitsinteressierte. Bemerkenswert ist der Versuch des Autors, zentrale und allgemeingültige Sicherheitsprinzipien herauszuarbeiten.

Impressum

http://www.secorvo-security-news.de

ISSN 1613-4311

Redaktion: Dirk Fox, Stefan Gora, Stefan Kelm, Jochen Schlichting

Herausgeber (V. i. S. d. P.): Dirk Fox
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses:
security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an
redaktion-security-news@secorvo.de

secorvo
security consulting

Secorvo Security News

Mai 2008

Editorial: Geistige Brandstifter

Der 11. September 2001 wird uns nicht nur als der Tag eines schockierenden Massenmords in Erinnerung bleiben. Er wird auch als Wendepunkt in die Annalen der Inneren Sicherheit eingehen. Mit beispielloser Geschwindigkeit zauberten Sicherheitsbehörden westlicher Regierungen gleich welcher politischen Couleur in den darauffolgenden Monaten neue Sicherheitsgesetze aus den Schubladen, die ohne nennenswerten politischen oder öffentlichen Widerstand die demokratischen Entscheidungsgremien passierten. Auch bestehende Befugnisse wurden ausgeweitet. In Deutschland stieg die ohnehin schon rekordverdächtig hohe Zahl angeordneter Telekommunikationsüberwachungen rapide: sie verdoppelte sich seit 2001 auf knapp 45.000 Fälle. 2007 war es für einen Bundesbürger 74 mal so wahrscheinlich, abgehört zu werden, wie für einen Nordamerikaner.

Erst in den vergangenen Monaten regt sich nennenswerter öffentlicher Widerstand – gegen die Pläne einer Online-Durchsuchung, den biometrischen Personalausweis und die Vorratsdatenspeicherung; ermutigt vom Bundesverfassungsgericht, das die rechtsstaatlichen Grenzen staatlicher Überwachung in Erinnerung gebracht hat.

Schlimmer noch als die schleichende Ausdehnung von Überwachungsbefugnissen ist jedoch der Geist, den die scheinbar widerspruchsfreie Beschränkung bürgerlicher Freiheitsrechte gesät hat. So sollte es eigentlich niemanden wundern, dass in der herrschenden Atmosphäre des Misstrauens Verantwortliche in Unternehmen auf die Idee kommen, Mitarbeiter, Aufsichtsräte und Investoren zu überwachen. Das Bewusstsein der Strafbarkeit solcher Maßnahmen kann in einem politischen Kontext abhanden kommen, in dem Datenschutz als „Täterschutz“ diffamiert wird, Abschüsse von Linienflugzeugen, Online-Überwachung und Vorratsdatenspeicherung ohne Rücksicht auf elementare Grundrechte in Gesetze gegossen werden und Nachrichtendienste rechtswidrig Journalisten bespitzeln. Die geistigen Brandstifter – die sitzen in den Innenministerien.

Inhalt

secorvo
security consulting

Security News

WLAN-Missbrauch strafbar

Erstmalig hat ein deutsches Gericht den Missbrauch eines ungeschützten privaten WLANs als Straftatbestand gewertet: Das Amtsgericht Wuppertal verurteilte in einem am 03.04.2008 publizierten Urteil (Az. 22 Ds 70 Js 6906/06) den „Schwarzsurfer" wegen unerlaubten Abhörens eines Funknetzes (§ 89 TKG) sowie nach § 44 BDSG wegen der widerrechtlichen Aneignung einer privaten IP-Adresse – die ihm der Router zugeteilt hatte. Die Strafe (20 Tagessätze) wurde zur Bewährung ausgesetzt, der Laptop des Täters jedoch als „Tatwerkzeug" eingezogen (NStZ 03/2008, S. 161 ff.). Auch wenn Kritik an der Rechtsauffassung des Gerichts angebracht erscheint, sollte man von der ungenehmigten Nutzung fremder WLANs tunlichst Abstand nehmen.

Botnetz-Analyse

Vitaly Kamluk, Virenanalyst bei Kaspersky Lab, veröffentlichte am 13.05.2008 eine lesenswerte Analyse über Botnetze. Neben einer systematischen Klassifizierung nach Architektur und verwendeten Netzprotokollen und einer anschaulichen Darstellung der Entwicklung der Botnetz-Technologie beleuchtet der Autor den gefährlichen Trend zu Peer-to-Peer-Botnetzen. Diese kommen ohne eine zentrale Kommandostelle aus, indem sie Befehle mit ihren „Nachbarn" austauschen. Besonders das „Sturmwurm"-Botnetz (SSN 08/2007) stellt eine erhebliche Bedrohung dar, da es sich über stündlich neue Mutationen verbreitet und bis zu seinem Einsatz unauffällig und „ruhig" verhält.

Die Analyse, die bei Kaspersky Lab auch als pdf-Datei heruntergeladen werden kann, schließt mit der Veranschaulichung einiger Geschäftsmodelle der „Botnetz-Industrie". Die zunehmende Professionalisierung von Konzeption, Infizierung und Steuerung von Zombie-PCs über Botnetze belegt, dass mit der Nutzung von Bots Geld verdient werden kann. Austrocknen lässt sich dieser Cyber-Sumpf nur an den Wurzeln: den Löchern in Systemen, die die Einnistung von Bots erst ermöglichen.

Schwerer Lotus Domino Bug

Am 20.05.2008 meldete MWR InfoSecurity einen Stack Overflow für IBMs Lotus Domino Web Server, der einem Angreifer die Ausführung beliebigen Codes unter System-Privilegien erlaubt – und der via Fernzugriff ausgelöst werden kann. Nachgewiesen wurde der Bug für die Versionen 7.0.3 und 8.0; mit hoher Wahrscheinlichkeit sind auch ältere Versionen betroffen. IBM hat passende Update-Patches bereitgestellt. Wer einen Lotus Domino Web Server im Internet betreibt sollte schnell reagieren.

Verbindungsdatenauskünfte

Neben den Inhalten unterliegen auch die „näheren Umstände" der Telekommunikation (Wer? Wo? Mit wem? Wann? Wie lange?), „Verbindungsdaten" genannt, dem Fernmeldegeheimnis (§ 88 TKG). Dessen Verletzung ist eine Straftat (§ 206 StGB) und kann mit bis zu fünf Jahren Freiheitsstrafe geahndet werden. Ausnahme: Strafverfolgungsbehörden dürfen im Zusammenhang mit Straftaten von „im Einzelfall erheblicher Bedeutung" (insbesondere die „Katalogstraftaten" des § 100a Abs. 2 StPO) auch ohne Wissen des Betroffenen Verkehrsdaten erheben (§ 100g StPO).

Das Max-Planck-Institut für ausländisches und internationales Strafrecht in Freiburg hat am 13.02.2008 ihre knapp 500 Seiten starke, im Auftrag des BMJ erstellte Langzeitstudie zur „Rechtswirklichkeit der Auskunftserteilung über Telekommunikationsverbindungsdaten nach §§ 100g, 100h StPO" vorgelegt. Danach ist die Zahl der Verkehrsdatenabfragen in den vergangenen Jahren explodiert: Waren es im Jahr 2000 noch 5.000, stieg die Anzahl 2005 auf das Achtfache (40.000 Abfragen). Eine wachsende Rolle spielen dabei offenbar Standort- und Funkzellenabfragen (18% bzw. 10%), mit denen der Aufenthaltsort Verdächtiger ermittelt werden kann – oder auch alle Personen, die sich zum Tatzeitpunkt mit eingeschaltetem Handy in einer bestimmten Funkzelle aufhielten.

Mängel stellt die Untersuchung insbesondere bei der Benachrichtigung der Betroffenen fest: lediglich in 4% der Fälle war die Benachrichtigung in den Akten dokumentiert; die Vernichtung der Daten konnte nur in 3% der untersuchten Verfahren den Akten entnommen werden. Wer mag sich da noch wundern, dass die derzeit vor dem Bundesverfassungsgericht verhandelte Vorratsdatenspeicherung von Verbindungsdaten Befürchtungen weckt?

Pseudozufall

Am 13.05.2008 veröffentliche das Debian Projekt eine korrigierte Version des OpenSSL-Packets, da alle OpenSSL-Versionen seit September 2006 (Versionen 0.9.8c-1 bis 0.9.8g-9) auf Debian-Distributionen wie Ubuntu kompromittierbare kryptografische Schlüssel erzeugen. Ursache: Die Funktion, die für zufällige Startwerte im Zufallszahlengenerator sorgen sollte, war im Quellcode auskommentiert. Der Zufallszahlengenerator nutzte daher die Linux Prozess ID als Zufallswert, die nur 32.767 mögliche

Werte annehmen kann. Daher lassen sich die geheimen Schlüssel von u.a. SSL, SSH, DNSSEC sowie X.509-Zertifikaten via Brute-Force-Angriff finden. Betroffen sind alle Programme, die OpenSSL zur Erzeugung kryptografischer Schlüssel verwenden, darunter Apache, Sendmail, Exim und OpenVPN.

Zweck der nicht mit dem OpenSSL-Entwicklungsteam abgestimmten Auskommentierung durch den Debian OpenSSL Maintainer war die Unterdrückung von Fehlermeldungen, die das Softwareanalysewerkzeug valgrind festgestellt und fälschlich als Softwarefehler interpretiert hatte. Da kommt der Draft der NIST-Publikation SP 800-108 „Recommendation for Key Derivation Using Pseudorandom Functions“ vom 01.05.2008 leider zu spät: Jetzt müssen zahlreiche Schlüssel getauscht werden – ein gutes Geschäft für Certificate Authorities.

Leitfäden zum “Hackerparagraf”

Am 17.04.2008 hatte die EICAR einen von Christian Hawellek und Dennis Jlussi von der Universität Hannover entwickelten Leitfaden zur strafrechtlichen Relevanz von IT-Sicherheitsaudits veröffentlicht, der Empfehlungen zur Durchführung von Audits im Kontext des neuen § 202c StGB (der „Hackerparagraf“, siehe SSN 07/2007) zusammenfasst. Er geht unter anderem ausführlich auf die Gestaltung von Einverständniserklärungen zur Vermeidung von Strafbarkeitsrisiken ein. Ebenfalls 16 Seiten umfasst der am 23.05.2008 vom Bitkom publizierte Praktische Leitfaden für die Bewertung von Software im Hinblick auf den § 202c, StGB. Neben einer Kriterienliste zur Beurteilung, ob eine Software unter die Bestimmungen des § 202c fällt, schlägt der Leitfaden „Best Practice“-Regelungen für den Umgang mit „Dual-Use“-Software im Unternehmen vor. Beide enthalten vernünftige Empfehlungen zur Absicherung, insbesondere im Falle einer externen Durchführung von IT-Sicherheitsaudits.

Malware mit Copyright

Am 25.04.2008 veröffentlichte Liam O. Murchu im Symantec Security Response Blog beispielhaft die Copyright- und Lizenzhinweise der ZeuS-Crimeware – eines russischen Malware-Construction-Kits zum Aufbau von Botnetzen. Darin droht der „Anbieter“ damit, jede nicht vertragskonforme Nutzung durch die Versendung der Signatur der spezifischen Binärdatei an führende Antiviren-Hersteller zu unterbinden. Eine interessante Rolle für die AV-Industrie – Copyright Enforcement für Schadsoftware-Baukästen. Möglicherweise kann sie sich dieser Rollenzuweisung nicht einmal entziehen.

Firewire macht Feuer

In der Theorie ist es ein alter Hut: Schon am 30.09.2006 hatte Adam Boileau auf der damaligen Ruxcon über Angriffe via Firewire vorgetragen. Seine ausführliche Präsentation „Hit by a bus: Physical Attacks with Firewire“ wurde damals von einer Live-Demo begleitet. Knapp zwei Jahre später nun unterlegt er seine akademische Attacke mit einem „Proof of concept“: Anfang März 2008 stellte Boileau das Tool winlockpwn auf seiner Website zur Verfügung. Mit diesem Tool kann von einem via Firewire verbundenen Computer ein Login an einem Rechner unter Windows XP (SP2) als Administrator erzwungen werden. Die erschreckende Eleganz dieses Angriffs lässt sich auf YouTube bewundern. Boileau nutzt dabei die Eigenschaft der Firewire-Schnittstelle, den Speicher des angeschlossenen Rechners direkt zu adressieren – und ihm so z.B. eine modifizierte DLL unterzuschieben.

Die Existenz von winlockpwn fordert in vielen Bereichen das Überdenken existierender Sicherheitskonzepte. Beispielhaft sei hier der – nicht zu empfehlende – Einsatz von Festplattenvollverschlüsselungslösungen ohne „Pre Boot Authentication“ genannt.

Secorvo News

Secorvo College aktuell

Die Nachfrage nach dem TISP-Zertifikat wächst ungebrochen: Schon weit über 200 deutsche Security Professionals dürfen sich mit diesem Titel schmücken, und 2008 werden voraussichtlich weitere 100 Absolventen das Zertifikat erwerben. Noch zwei letzte freie Plätze für Kurzentschlossene gibt es auf dem TISP-Seminar am **02.-06.06.2008**.

Die nächste Gelegenheit zur TISP-Zertifizierung bietet College nach der Sommerpause vom **08.-12.09.2008**. Vorher führt College vom **01.-03.07.2008** noch mit einem dreitägigen Seminar in die Durchführung von forensischen Analysen ein.

Security Awareness Symposium

Vom 17.-18.06.2008 findet das sechste „Security Awareness Symposium“ statt, das sich zum jährlichen Treffpunkt von Security-Awareness-Verantwortlichen entwickelt hat. Auf dem von Secorvo zusammen mit den E-Learning-Experten von digital spirit und der Agentur DauthKaun veranstalten Symposium in den stilvollen Räumen der Buhlschen Mühle in Ettlingen werden unter anderem die Erfahrungen der Münchener Rück, SAP, T-Systems und MDS vorgestellt und diskutiert.

Veranstaltungshinweise

Auszug aus http://www.veranstaltungen-it-sicherheit.de

Mai 2008	
29.05.	Pimp your web (KA-IT-Si, Karlsruhe)
Juni 2008	
02.-06.06.	T.I.S.P.-Schulung (Secorvo College)
09.-10.06.	DuD 2008 (Computas, Berlin)
17.-18.06.	6. Security Awareness Symposium (Secorvo, Karlsruhe-Ettlingen)
24.-25.06.	D-A-CH Security 2008 (GI/OCG/Bitkom/TTT, Berlin)
24.-26.06.	Sichere Softwareentwicklung (Secorvo College)
Juli 2008	
01.-03.07.	Forensik (Secorvo College)
10.-11.07.	DIMVA 2008 (GI)
28.07.-1.08.	17th USENIX Security Symposium 2008 (San José/US)
August 2008	
17.-21.08.	Crypto 2008 (IACR, Santa Barbara/US)

Fundsache

Symantec hat am 08.04.2008 den 13. „Global Internet Thread Report" für den Sechsmonatszeitraum Juli bis Dezember 2007 publiziert. Er enthält eine umfangreiche Analyse der Entwicklung aktueller Bedrohungen durch Malware, Botnetze und sicherheitskritische Softwarefehler. Explodiert ist die Menge bösartigen „Malicious Code": Gegenüber dem Vorjahreszeitraum hat sich deren Zahl auf 500.000 mehr als versechsfacht.

Impressum

http://www.secorvo-security-news.de

ISSN 1613-4311

Redaktion: Dirk Fox, Kai Jendrian, Jochen Schlichting

Herausgeber (V. i. S. d. P.): Dirk Fox
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses:
security-news@secorvo.de
(Subject: „subscribe security news")

Wir freuen uns über Ihr Feedback an
redaktion-security-news@secorvo.de

secorvo
security consulting

SSecorvo Security News

Juni 2008

Editorial: Reden ist Silber

Schweiger erfreuen sich in westlichen Gesellschaften eines guten Rufs. Wer wenig redet, den umgibt der Nimbus des Vergeistigten – denn „Stille Wasser sind tief", wie der Volksmund weiß. Oder er gilt gar als weise: Von Ernest Hemingway (1899-1961) ist der Ausspruch überliefert, man brauche „zwei Jahre, um sprechen zu lernen, und fünfzig, um schweigen zu lernen". Zumeist gilt Schweigen als ein Indiz für Nachdenken – wenigstens bis zum Beweis des Gegenteils: „Wo Männer schweigen, reden die Gedanken" (Carl Spitteler, 1845-1924).

Nicht immer aber stimmt das Klischee. Denn Schweigen kann auch mehr Schein als Sein verbergen. Das wird oft erst deutlich, wenn sich ein stilles Wasser als seichte Pfütze outet. Ein fast 1.500 Jahre altes Bonmot belegt die lange Tradition des Schweigens als potemkinsches Dorf: „Si tacuisses, philosophus mansisses" reimte der Philosoph Boethius (ca. 475–525 n. Chr.) – „Hättest Du geschwiegen, wärst Du Philosoph geblieben." Die Motivation des taktischen Schweigens hat der französische Schriftsteller François Duc de La Rochefoucauld (1613-1680) auf den Punkt gebracht: „Schweigen ist der beste Ausweg für den, der seiner Sache nicht sicher ist." Bei hartnäckigem Schweigen ist daher Vorsicht angeraten.

Die Geschichte der Kryptographie kennt unzählige Beispiele für dünne Bretter, die allein durch Schweigen hielten: Crypto-1 (Mifare) und KeeLoq sind zwei der jüngsten. Auch wenn es immer wieder behauptet wird: Die Sicherheit eines (Krypto-)Verfahrens steigt nicht durch Geheimhaltung. Im Gegenteil: „Security by Obscurity" erhöht das Risiko eines schlagartigen Sicherheitsverlustes, falls das Verfahren bekannt wird. Immer wieder bestätigt sich der von Auguste Kerckhoffs vor 125 Jahren in „La Cryptographie Mililtaire" formulierte Fundamentalsatz der modernen Kryptographie: Die Sicherheit eines kryptographischen Mechanismus' darf nur von der Geheimhaltung des Schlüssels abhängen. Oder kurz: Reden ist Silber. Schweigen ist ... Mist. Zumindest in der Kryptographie.

Inhalt

secorvo
security consulting

Security News

OpenSSL Nachwehen

Die meisten Probleme des am 13.05.2008 bekannt gewordenen Sicherheits-Desasters von OpenSSL in Debian-basierten Linux-Distributionen sind umfänglich beschrieben und diskutiert worden (siehe auch SSN 05/2008). Möglicherweise betroffene Server-Schlüssel können seit dem 09.06.2008 mit dem SSL-Online-Check des Heise-Verlags überprüft werden.

Auf ein etwas vernachlässigtes Risiko wollen wir jedoch hinweisen: Auch Schlüssel, die auf Systemen erzeugt wurden, die von der OpenSSL-Problematik nicht betroffen waren, müssen als kompromittiert gelten, wenn sie auf einem betroffenen System zur Public-Key-Authentifizierung mit DSA, wie z. B. bei SSH, eingesetzt wurden. DSA benötigt zum Signieren eine vom Client-System erzeugte Zufallszahl, die geheim bleiben muss. Mit Kenntnis dieser Zufallszahl kann mit einfacher Mathematik in wenigen Schritten der private Schlüssel aus einer veröffentlichten DSA-Signatur herausgerechnet werden. Noch einfacher ist es bei einem Diffie-Hellman-Schlüsselaustausch: Die kleine Menge möglicher Zufallszahlen auf einem betroffenen Client erlaubt es einem Angreifer, mit begrenztem Aufwand den Session-Key aus mitgeschnittenen SSH-Sessions zu gewinnen.

ISO-Risikomanagement

Mit dem am 04.06.2008 veröffentlichten Standard ISO/IEC 27005:2008 "Information technology – Security techniques – Information security risk management" hat die ISO die Normenreihe ISO/IEC 2700x um einen wichtigen Baustein ergänzt. Neben einer verallgemeinerten Herangehensweise an das Thema Risikomanagement werden darin wesentliche Prozessschritte wie beispielsweise die Risiko-Identifikation, -Bewertung und -Akzeptanz beschrieben und konkrete Hilfestellung zur Anwendung gegeben. Der neue Standard konkretisiert damit die Anforderungen an das Risikomanagement aus ISO/IEC 27001:2005.

Cisco Rootkits

Am 22.05.2008 stellte Sebastian Muniz auf der EuSecWest in London ein funktionsfähiges Rootkit für Cisco IOS vor. Dessen Wirksamkeit wurde inzwischen durch eine offizielle Stellungnahme des Herstellers bestätigt. Einen Tag zuvor hatte Cisco drei außerplanmäßige Patches veröffentlicht, die mit der IOS-Rootkit-Thematik zusammenhängen dürften. Insbesondere der Cisco IOS SSHService Denial of Service-Fehler wird als reengineer-bar eingestuft, daher sollte mit Angriffen auf diese Schwachstelle gerechnet werden. Wir empfehlen, betroffene Systeme umgehend zu patchen.

Automatische Exploits

David Brumley, Pongsin Poosankam, Dawn Song, und Jiang Zheng veröffentlichten am 18.04.2008 einen Ansatz zur automatischen Erzeugung von Exploits aus Patches. Die Kernidee: Sie vergleichen das gepatchte mit dem ursprünglichen Programm. Identifizieren sie dabei beispielsweise eine Input-Validierung, so erzeugen sie daraus Angriffscode, der gegen genau diese Validierung verstößt – und können nun jedes ungepatchte System attackieren. Zwar lassen sich mit diesem Ansatz (noch) nicht alle Exploits zu jedem Patch finden; für ausgewählte Microsoft-Patches konnten sie jedoch in weniger als 30 Sekunden funktionsfähige Exploits gewinnen. Sollte dieser Ansatz weiter entwickelt werden, könnten Hersteller und Anwender in Zugzwang geraten und müssten sich um geeignete Gegenmaßnahmen und zügigeres Patchen bemühen.

PTK Forensics

Seit dem 30.05.2008 läuft der öffentliche Beta-Test für PTK – eine neue, völlig überarbeitete graphische Benutzeroberfläche für das altehrwürdige Forensik-Tool The Sleuthkit (TSK). Dabei handelt es sich nicht bloß um eine aktuellere Version der bereits etwas in die Tage gekommenen Sleuthkit-Benutzeroberfläche Autopsy. Die Entwickler der italienischen DF LABS srl wollten vielmehr komplett neue Funktionen zur Verfügung stellen.

Wir haben das Tool einem ausgiebigen Test unterzogen. Vor der eigentlichen Analyse extrahiert die neue "Indexing Engine" Textpassagen, sucht nach bekannten Dateitypen, führt File-Carving durch, berechnet bei Bedarf kryptographische Prüfsummen und legt die Ergebnisse in einer SQL-Datenbank ab. Anschließend kann der Forensiker über eine Ajax-basierte Web-Schnittstelle auf zahlreiche Funktionen zugreifen. Dabei überzeugen Features wie die "Gallery", die eine Vorschau auf gefundene Bilder erlaubt, oder eine nützliche "Bookmark"-Funktion zur Hervorhebung wichtiger Suchtreffer.

Der Beta-Test läuft bis September 2008. Da es gelegentlich zu Fehlermeldungen kommt und noch nicht alle Funktionen aus TSK und Autopsy implementiert sind, stellt PTK zur Zeit noch keinen vollwertigen Ersatz dar.

Exponierte Leittechnik

Nun ist es ja nicht so, dass analoge Leittechnik unangreifbar wäre: Ein durchgetrenntes Kabel kann die Verfügbarkeit von Anlagen gefährden, und das

Drehen an einem Potentiometer könnte Signale verfälschen. Allein der Umstand, dass man hierzu einen physikalischen Zugriff vor Ort benötigt, erschwert derartige Angriffe erheblich. Anders sieht es dagegen bei der digitalen Leittechnik aus: Durch TCP/IP verbundende Systeme können über hunderte von Kilometern hinweg beeinflusst werden.

Schutz bieten hier durchdachte Netzwerk-Zonenkonzepte und entsprechend restriktiv konfigurierte Firewalls. Dass es daran gelegentlich mangelt, zeigen die Feststellungen der US-amerikanischen Überwachungsbehörde Government Accountability Office (GOA) bei einem der größten Energieversorger, der Tennessee Valley Authority (TVA); nachlesbar in einem Prüfbericht vom 21.05.2008. Darin werden unter anderem Verbindungen zwischen Anlagennetzen und Office-Netzsegmenten und zu offen konfigurierte Firewallsysteme bemängelt. Kein Wunder, dass in den USA die Angst vor einem Hacker-Angriff auf die Energieversorgung umgeht.

Reaktorabschaltung per Patch

Am 05.06.2008 wurde ein peinlicher Zwischenfall in einem amerikanischen Atomkraftwerk bekannt: Ein Service-Techniker hatte im Kraftwerk Hatch auf einem PC im Office-Netzsegment ein Update installiert, das durch eine fehlerhafte Synchronisierung Daten auf einem Kontrollsystem im Anlagennetz löschte. Die fehlenden Daten wurden von den Schutzsystemen des Reaktors als zu niedriger Kühlwasserstand interpretiert – und daher eine Notabschaltung ausgelöst, so die Darstellung im NRC-Bericht (Nuclear Regulatory Commission).

Zwar ist zu hoffen, dass ein solcher Vorfall in einem deutschen Kraftwerk nicht möglich wäre. Aber beunruhigend ist auch schon die Vorstellung, dass ein einfaches Systemupdate solche Aktionen auslösen kann – selbst bei einem 7.400 km entfernten Kernkraftwerk.

Nessus-Lizenz

Der Security-Scanners Nessus, einstmals Open Source, seit 2005 als Closed Source weiterentwickelt (vgl. SSN 02/2005), erfreut sich auch in Unternehmen großer Beliebtheit. Mit dem bisherigen Nutzungsmodell, nach dem Updates und Plugins mit etwas Verzögerung kostenfrei zum Download bereitgestellt wurden, ist es für den kommerziellen Einsatz am 31.07.2008 vorbei: In einem Schreiben informierte der Hersteller Tenable registrierte Nutzer am 14.05.2008 über die bevorstehenden Änderungen der Lizenzbedingungen.

Ab dem 01.08.2008 ist nur noch die private Nutzung kostenfrei. Auf die Reaktion der Nessus-Fangemeinde darf man gespannt sein. Vielleicht hätte Tenable lieber die Reaktion des Marktes auf die am 06.06.2008 angekündigte 33%ige Preiserhöhung des Kultgetränks Bionade (um sich so „von seinen Nachahmern abzusetzen“) abgewartet – schließlich lernt man immer am billigsten aus den Fehlern anderer. Die Kommerzialisierung von Nessus dürfte dem vom BSI unterstützen und am 21.05.2008 auf dem LinuxTag 2008 vorgestellten Projekt OpenVAS Vortrieb leisten: einem auf Basis der letzten frei verfügbaren Quellen von Nessus entwickelten kostenfreien Security-Scanner.

Secorvo News

Secorvo College aktuell

Vom **01.–03.07.2008** entführen Stefan Kelm, Stefan Gora und Jochen Schlichting in die Tiefen der Forensik – inklusive praktischer Übungen an elementaren Tools und einer Einführung in den rechtlichen Kontext. Der Termin ist seit einigen Wochen ausgebucht – die nächste Gelegenheit zur Teilnahme bietet sich am **11.–13.11.2008**. Interessierten empfehlen wir eine frühzeitige Anmeldung.

Das Programm des zweiten Halbjahrs beginnt nach der Sommerpause mit einer T.I.S.P.-Schulung vom **08.–12.09.2008** mit anschließender Zertifizierung. Die große Nachfrage nach dem T.I.S.P.-Zertifikat lässt erwarten, dass sich die Zahl der Absolventen in 2008 erneut verdoppelt.

Programm und Online-Anmeldung unter
http://www.secorvo.de/college

Team(ver)stärkung

Das Secorvo-Team ist zum 01.06.2008 weiter gewachsen: Alexander Göbel – T.I.S.P., CISM, CISO und BSI-zertifizierter Audit-Teamleiter für ISO 27001-Audits auf der Basis von IT-Grundschutz – bringt vieljährige Erfahrung aus dem IT-Risk-Management eines DAX-Unternehmens und der Zertifizierung eines Rechenzentrums nach ISO 27001 auf der Basis von IT-Grundschutz mit. Neben allen Facetten des Sicherheitsmanagements ist der betriebliche Datenschutz eines seiner Schwerpunktthemen.

Ebenfalls gewachsen ist die inzwischen lange Liste der Zertifizierungen der Secorvo-Consultants: Petra Barzin erhielt die Zertifizierung als CISSP, und Jochen Schlichting darf neben seinen Zertifizierungen als CISA und CISSP nun auch das CISM-Zertifikat (Certified Information Security Manager) der ISACA führen.

Veranstaltungshinweise

Auszug aus http://www.veranstaltungen-it-sicherheit.de

Juli 2008	
01.-03.07.	Forensik (Secorvo College)
10.07.	Die Mifare-Attacke und andere Krypto-Desaster (KA-IT-Si, Karlsruhe)
10.-11.07.	DIMVA 2008 (GI, Paris)
28.07.-01.08.	17th USENIX Security Symposium 2008 (Usenix, San José/US)
August 2008	
17.-21.08.	Crypto 2008 (IACR, Santa Barbara/US)
September 2008	
07.-10.09.	OSSCoNF 08 (IFIP, Mailand)
08.-12.09.	T.I.S.P.-Schulung (Secorvo College)
23.-25.09.	IMF 2008 (GI, Mannheim)
23.-26.09.	PKI – Grundlagen, Vertiefung, Realisierung (Secorvo College)
Oktober 2008	
07.-10.10.	IT-Sicherheit heute (Secorvo College)

Fundsache

Am 09.05.2008 veröffentlichte die schweizerische Melde- und Analyse-stelle Informationssicherung (Melani) den Halbjahresbericht 2007/2, der die Entwicklung der Gefährdungslage in der Schweiz und international beleuchtet. Als Beispiel wird ein sehr professioneller Phising-Angriff auf Systeme der Schweizer Bundesverwaltung detailreich dargestellt – der die Wirkungslosigkeit des etablierten Virenschutzes aufzeigte.

Impressum

http://www.secorvo-security-news.de

ISSN 1613-4311

Redaktion: Dirk Fox, Stefan Gora, Kai Jendrian, Stefan Kelm, Jochen Schlichting

Herausgeber (V. i. S. d. P.): Dirk Fox
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses:
security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an
redaktion-security-news@secorvo.de

secorvo
security consulting

Secorvo Security News

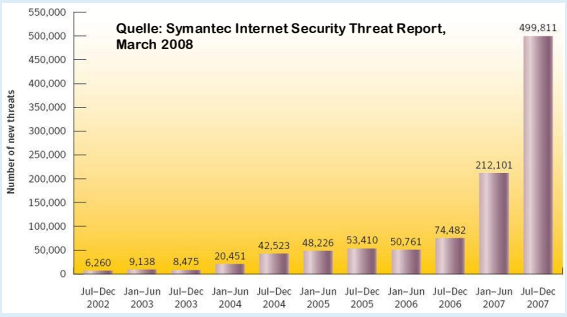
Juli 2008

Editorial: Geburtstagstorte

Wer Kinder hat, kennt Pettersson und Findus – den alten, schrulligen, liebenswerten Bauern mit seinem quirligen sprechenden Kater in grüner Hose, detailreich gezeichnet von Sven Nordqvist. „Eine Geburtstagstorte für die Katze“ heißt das 1984 erschienene erste Bilderbuch der Kultserie. Die Geschichte ist fix erzählt: Findus beschließt, Geburtstag zu haben – denn dann gibt es Pfannkuchentorte. Das ist jedoch leichter gesagt als getan: Das Mehl ist ausgegangen, und das Fahrrad hat einen Platten. Pettersson muss es reparieren, bevor er zum Einkaufen fahren kann – das Werkzeug aber liegt im verschlossenen Schuppen, und den Schlüssel entdeckt Findus im Brunnen. Um ihn herauszufischen braucht er die Angel vom Dachboden, aber an der Leiter lehnt ein schlafender Stier. Also muss Findus mit einer Gardine den Matador geben, reißt aber dabei den Eierkorb um.

Natürlich kommt der Kater doch noch zu seiner Geburtstagstorte. Aber das war jedenfalls für meine Kinder ganz unwichtig – gebannt verfolgten sie die immer neuen Widrigkeiten und deren kreative Beseitigung. Der Umweg war das Ziel, und die Torte bestenfalls die Belohnung für die erfolgreiche Problemlösung.

Sehr ähnlich müssen die Autoren von Malware empfinden. Wie anders ist zu erklären, dass sie sich weder von immer besseren Schutzmaßnahmen noch von schärferen Strafgesetzen abschrecken lassen? Statt dessen ersinnen sie raffiniertere Angriffsmethoden. Offenbar spornt der Widerstand an, das belegen die Zahlen. Und dahinter steht heute meist ein Investor, der auf die Torte scharf ist.



Inhalt

secorvo
security consulting

Security News

BSI-Krypto-Richtlinie

Seit Inkrafttreten des deutschen Signaturgesetzes vor mehr als 10 Jahren erstellt das BSI jährlich eine aktuelle Übersicht geeigneter kryptographischer Algorithmen und Schlüssellängen für digitale Signaturen. Verschlüsselungsverfahren spielen darin naturgemäß keine Rolle – gleichwohl sind sie in der Praxis viel verbreiteter als digitale Signaturen.

Mit der Veröffentlichung einer technischen Richtlinie „Kryptographische Verfahren: Algorithmen und Schlüssellängen“ (TR 02102) hat das BSI am 20.06. 2008 nun auch bei Verschlüsselungsverfahren, Authentisierungsmechanismen, Zufallszahlengeneratoren und Schlüsselvereinbarungsprotokollen Farbe bekannt. Eine wertvolle Orientierung für die Praxis.

Survival of the Fittest

Am 14.07.2008 veröffentlichte Torsten Holz in seinem Blog die Ergebnisse einer 12monatigen Honeynetanalyse zur Überlebenszeit ungepatchter IT-Systeme. Untersucht wurde die Dauer einer erfolgreichen Kompromittierung durch autonome Malware, die alte, lange bekannte Schwachstellen ausnutzen. Ergebnis: Im Schnitt überlebt ein System ca. 12 Minuten, etwas länger als die vom Internet Storm Center gemessenen knapp fünf Minuten.

Die Analyse, die auf den Vorarbeiten von Laura Itzel aufbaut, weist eine erhebliche Abhängigkeit der Überlebenszeit vom jeweiligen Internet Service Provider nach: ISPs, die bevorzugt von Malware genutzte Ports sperren, erhöhen die Überlebenszeit angeschlossener Systeme um ein Vielfaches. Angesichts des deutlich größeren Zeitfensters zwischen Bekanntwerden einer Schwachstelle und Verfügbarkeit des Patches („Window of Exposure“) erscheint es jedoch in keinem Fall angeraten, eine Internet-Verbindung ohne gut konfigurierte Personal Firewall aufzubauen.

Schlecht versteckt

Dass Blicke über den Tellerrand auch in der Kryptographie wichtig sind, belegt eine Arbeit, die Forscher der University of Washington zusammen mit Bruce Schneier am 29.07.2008 auf einem USENIX Workshop vorgestellt haben. Darin untersuchten sie die Sicherheit von „Deniable File Systems“, mit deren Hilfe die Existenz verschlüsselter Daten verschleiert werden soll – beispielsweise mit „Hidden Volumes“ des Verschlüsselungstools TrueCrypt. Aber auch versteckte Dateisysteme hinterlassen im Betriebssystem unvermeidlich Spuren, wenn sie aktiviert werden, z. B. als kürzlich geöffnete „Recent Items“. Im schlimmsten Fall findet sich, lange nach der Deaktivierung des „Hidden Volumes“, Klartext-Inhalt einer versteckten Datei im Cache von Google-Desktop.

Was des einen Leid, ist des anderen Freud’ – die Forensiker reiben sich die Hände. Einige der aufgedeckten Probleme wurden in der am 06.07.2008 erschienenen Version 6 von TrueCrypt behoben.

Evilgrade

Am 28.07.2008 veröffentlichte Francisco Amato das Framework Evilgrade. Der Schadsoftware-Baukasten nutzt als Verbreitungsmechanismus verbreitete Updatemechanismen und tarnt sich als automatischer Patch. Derzeit werden u.a. Java Plugins, Winzip, Winamp und iTunes simuliert; Schadcode kann für beliebige Zielplattformen ergänzt werden. Die Integration der am 08.07.2008 von Dan Kaminsky publizierten DNS Cache Poisoning Variante in das Metasploit-Attackframework vereinfacht die Anwendbarkeit von Evilgrade erheblich – und macht es sehr gefährlich: Fast alle DNS-Server waren bzw. sind ohne aktuelle Updates von dieser Schwäche betroffen. Wer nicht Teil des Problems sein möchte, sollte schnell patchen.

CrypTool 1.4.2x

Fast genau ein Jahr nach der Veröffentlichung von Version 1.4.10 ist am 11.07.2008 CrypTool als neues Release 1.4.21 erschienen. Neben vielen kleinen Korrekturen und akribischer Detailpflege an Bedienungsfreundlichkeit und Dokumentation wurden der Passwort-Qualitätsmesser optimiert und die Hashfunktionenfamilie SHA-2 integriert. Der Passwort-Generator erzeugt zufällige Passworte aus einem voreinstellbaren Alphabet – auch für WLANs.

Besonders erwähnenswert ist die jüngste Auszeichnung des Open Source Projekts: In einer Festveranstaltung wurde CrypTool am 22.07.2008 an der Uni Siegen im Rahmen der Kampagne „Deutschland Land der Ideen“ als „Ausgewählter Ort 2008“ ausgezeichnet.

BSI-Standards 2.0

Am 23.06.2008 hat das Bundesamt für Sicherheit in der Informationstechnik (BSI) die zweite Auflage der überarbeiteten BSI-Standards 100-1 „Managementsysteme für Informationssicherheit“, 100-2 „IT-Grundschutz-Vorgehensweise“ und 100-3 „Risikoanalyse auf Basis von IT-Grundschutz“ veröffentlicht. Diese drei Standards bilden die Grundlage für den nach ISO 27001 ausgerichteten IT-Grundschutz. Die Neuauflage verschiebt den Blickwinkel von der reinen IT-Sicherheit zur Informationssicherheit; außerdem wurden die Standards um Datenschutzaspekte erweitert. Und schließlich wurde die

Fortschreibung der relevanten ISO-Standards der 2700x-Reihe berücksichtigt. Der neue BSI-Standard 100-4 zum Notfall-Management liegt nach wie vor nur als Entwurf vor.

Bluetooth Security

Zwar ist Bluetooth schon lange keine neue Technik mehr – kaum ein IT-Gerät, das etwas auf sich hält, kommt noch ohne daher. Und obwohl Security-Mechanismen und potentielle Schwachstellen schon lange dokumentiert sind, kommt es immer wieder zu fehlerhaften Implementierungen – Handys, die sich via Bluetooth Malware einfangen oder ferngesteuert werden können, oder Headsets, die aus der Ferne als Überwachungsmikrofon missbraucht werden können. Mit den 2004 und 2005 entwickelten Tools der trifinity-Gruppe – darunter Bluebug, Bluesnarf, Blueprint, Bluedump und Car Whisperer – ist das bei betroffenen Systemen ein Kinderspiel.

Nun hat offenbar auch das US-amerikanische NIST gemerkt, dass hier ein reales Risiko steckt und am 09.07.2008 einen Guide to Bluetooth Security (Draft SP 800-121) publiziert – mit der Bitte um Kommentierung bis 22.08.2008. Eine nette Urlaubslektüre ...

Link-Prefetching im Firefox

Nicht neu, aber nicht überall bekannt: Im Mozilla-Browser Firefox ist die Funktion Link-Prefetching in den Voreinstellungen aktiviert. Webseiten, die diese Funktion zum Einbinden von Links verwenden, sorgen dafür, dass die Inhalte der Links schon im Voraus geladen werden, ohne dass der Nutzer den Link angeklickt hat – in der Regel merkt er davon nicht einmal etwas.

Dafür liegt der möglicherweise rechtswidrige Inhalt der verlinkten Seite im Cache. Auch aus Sicherheitsperspektive ist diese Funktion nicht unbedenklich: Da sich Trojaner angesichts immer wirksamerer Spam- und Virenscanner in wachsendem Umfang über präparierte Webseiten statt per E-Mail verbreiten, können Angreifer Prefetching-Links auf eine einzige mit Schadcode versehene Webseite auf vielen unzureichend geschützten Seiten Dritter verstecken und so zahlreiche Systeme unbemerkt infizieren. Vorteil für den Angreifer: Schadcode-Updates muss er nur auf einer Webseite einspielen, und zur Spurenverwischung genügt die Entfernung genau dieses Codes. Abhilfe ist jedoch einfach: Zum Deaktivieren muss unter der URL „about:config“ der Wert des Parameters „network.prefetch-next“ durch Anklicken von true auf false gesetzt werden.

WAF-Pflicht

Die Anforderungen des Payment Card Industry (PCI) Data Security Standard V.1.1 vom 15.04.2008 an den Schutz von Web-Applikationen (Abschnitt 6.6) sind seit dem 30.06.2008 keine Empfehlung mehr, sondern eine verbindliche Vorgabe: Code-Reviews, eine automatisierte Schwachstellen-Analyse und die Nutzung von Web Application Firewalls (WAF) sind nunmehr Pflicht. Ein ergänzendes Dokument des PCI Security Standards Council erläutert die Anforderungen stichwortartig auf wenigen Seiten – für einige Anbieter sicher eine Herausforderung.

Secorvo News

Secorvo College aktuell

Nach der Sommerpause startet das Programm von Secorvo College am **08.–12.09.2008** mit einer T.I.S.P.-Schulung in das zweite Halbjahr – gefolgt von einer komplett unabhängigen Zertifikats-Prüfung durch iSQI am 13.09.2008 in den Räumen von Secorvo. Es folgt ein Klassiker in aktuellem Gewand: PKI – Grundlagen, Vertiefung, Realisierung am **23.–25.09. 2008** – baldige Anmeldung empfohlen.

Schon jetzt möchten wir Sie auf unser Forensik-Seminar vom **11.–13.11.2008** hinweisen. Die „Premiere“ im Juli war ausgebucht – und wurde von den Teilnehmern euphorisch gelobt („Mit dem Seminar hat sich Secorvo selbst übertroffen. (...) Ich kann jedem, der mit IT-Security zu tun hat, dieses Seminar nur wärmstens empfehlen. Drei Tage voller Information, Spannung, Überraschungen, Aha-Effekte und optimaler Mischung aus Theorie und Praxis.“ – Matthias Grund, Siemens AG).

Termine, Programme und Online-Anmeldung unter http://www.secorvo.de/college

Symposium Wirtschaftsspionage

Schutzmassnahmen gegen die ungezielte Bedrohung durch Schadsoftware und Hacker sind bei Unternehmen heute eine Selbstverständlichkeit. Seit etwa zwei Jahren belegen Studien jedoch einen unheilvollen Trend: Im Schatten wachsender Spam- und Trojaner-Wellen nehmen gezielte Spionageattacken zu – nicht nur unter Nutzung technischer Hilfsmittel.

Das "Symposium Wirtschaftsspionage" von Econo und Secorvo wird sich am **03.09.2008** diesem Thema widmen. Ulf Tietge, Chefredakteur von Econo, wird das Symposium moderieren, auf dem sowohl Fachexperten (u. a. Dr. Udo Ulfkotte und Hans Schlumpberger vom Landesamt für Verfassungsschutz BaWü) als auch Unternehmen die tatsächliche Bedrohungslage analysieren und ihre Schutzmaßnahmen vorstellen (vollständiges Programm, Online-Anmeldung und Anfahrtskizze).

Veranstaltungshinweise

Auszug aus http://www.veranstaltungen-it-sicherheit.de

August 2008	
17.-21.08.	Crypto 2008 (IACR, Santa Barbara/US)
September 2008	
03.09.	Symposium Wirtschaftsspionage (Secorvo, Ettlingen)
08.-12.09.	T.I.S.P.-Schulung (Secorvo College)
23.-26.09.	PKI – Grundlagen, Vertiefung, Realisierung (Secorvo College)
23.-25.09.	IMF 2008: 4th International Conference on IT-Incident Management & IT-Forensics (GI, Mannheim)
Oktober 2008	
07.-09.10.	ISSE 2008 (EEMA/TeleTrusT, Madrid/ES)
07.-10.10.	IT-Sicherheit heute – Angriffe, Konzepte, Lösungen (Secorvo College)
28.-30.10.	IT-Sicherheitsaudits in der Praxis – Konzeption, Durchführung, Bewertung (Secorvo College)

Fundsache

Das Verizon Business RISK Team hat im 2008 Data Breach Investigations Report die Ergebnisse seiner forensischen Analysen der letzten vier Jahre ausgewertet und zusammengefasst. Dabei wurde neben der Komplexität der Angriffe analysiert, wie der Datendiebstahl zu Stande kam und wer der Urheber war. Abweichend von der verbreiteten Überzeugung, dass Insider die meisten Angriffe verursachen, zeigt die Auswertung, dass in fast 80% der untersuchten Fälle der Zugriff von außen erfolgte, dabei allerdings häufig Geschäftspartner involviert waren.

Impressum

http://www.secorvo-security-news.de

ISSN 1613-4311

Redaktion: Dirk Fox, Stefan Gora, Kai Jendrian,
Hans-Joachim Knobloch, Natalie Mareth, Jochen Schlichting

Herausgeber (V. i. S. d. P.): Dirk Fox
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses:
security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an
redaktion-security-news@secorvo.de

secorvo
security consulting

Secorvo Security News

August 2008

Editorial: Vom Urteilen

Ein Urteil, so die eingängige Definition in Wikipedia, ist „eine wertende Entscheidung über einen Sachverhalt oder Erkenntnisgegenstand". Entscheidungen zwischen alternativen Bewertungsmöglichkeiten treffen wir ständig – mit mehr oder weniger guter Kenntnis der Zusammenhänge. Viele unserer Urteile sind daher genau besehen Vorurteile, also eine „im Allgemeinen wenig reflektierte Meinung – ohne vollständige Würdigung aller relevanten Eigenschaften eines gewerteten Sachverhalts oder einer Person". Vorurteile sind voreilige Urteile, sie verallgemeinern ohne Berücksichtigung des Einzelfalls.

Das ist nicht notwendig schlecht und manchmal überlebenswichtig. Für viele unserer wertenden Entscheidungen steht uns zu wenig Zeit zur Verfügung, um den Sachverhalt angemessen zu analysieren. Vorurteile geben eine (erste) Orientierung und erlauben sofortiges Handeln. Dabei müssen wir uns aber bewusst machen, dass das Vorurteil nur ein vorläufiges Urteil sein kann, das durch zusätzliche Informationen oder Erkenntnisse in ein reiferes münden sollte.

Die „vollständige Würdigung aller relevanten Eigenschaften" erfordert Disziplin, Zeit und die Offenheit für die Revision eines (Fehl-)Urteils. Daher wurde für Urteile mit besonderer Tragweite für Betroffene das Amt des Richters geschaffen und die Möglichkeit zur Revision institutionalisiert. Im Finanzwesen ist derzeit jedoch ein Trend zur vermeintlichen Objektivierung von z. B. Kreditentscheidungen durch den Rückgriff auf personenbezogene Informationen Dritter zu beobachten, verschleiernd „Rating" genannt. Verständlich vielleicht, dass ein Online-Anbieter nicht gegenüber einem notorischen Zahlungsverweigerer in Vorleistung gehen möchte. Aber soll eine Bank die Kreditbedingungen verschärfen dürfen, weil ein direkter Verwandter des Kunden Privatinsolvenz angemeldet hat? Oder einen Kredit verweigern, weil der Kunde in einem schlecht beleumundeten Viertel wohnt? Da fehlt nicht viel, und aus „automatisierten Einzelentscheidungen" werden nicht-revidierbare Vorurteile – und damit gesamtgesellschaftliche Freiheitsbegrenzer.

Inhalt

secorvo
security consulting

Security News

Rutkowska strikes again

Die auf virtuelle Rootkits spezialisierte Forscherin Joanna Rutkowska hat wieder zugeschlagen: Auf der diesjährigen Blackhat stellte sie am 07.08.2008 mit ihren Kollegen Rafal Wojtczuk und Alexander Tershkin vor, wie man den Hypervisor der Virtualisierung Xen mit Rootkits trojanisieren kann. Die technischen Details sind anspruchsvoll und interessant: Der modifizierte Code wird dem bereits laufenden Hypervisor über eine Netzwerkkartentreiber-Software oder den Festplattencontroller untergeschoben und im laufenden Betrieb über Direct Memory Access (DMA) zur Ausführung gebracht.

Wie bereits bei ihrem 2006 vorgestellten Rootkit BluePill (siehe SSN 8/06), das die Virtualisierungsfunktionen von AMD-Prozessoren nutzt, ist die Erkennung dieser Angriffssoftware sehr schwierig. Derzeit entwickeln Rutkowska und ihre Kollegen im Projekt HyperGuard die BIOS-Funktionen von Mainboards weiter, um einen Integritätsschutz der Hypervisor-Software zu ermöglichen – damit wäre wirksame Abhilfe möglich.

Schwachstellen-Primus Browser

In einer am 14.08.2008 vom Deutschen Sicherheitsnetz e.V. vorgestellten Untersuchung wurde festgestellt, dass von 253 geprüften privaten PC-Systemen gut die Hälfte Browserschwachstellen aufwies. Deutlich repräsentativer, aber im Ergebnis vergleichbar sind die am 10.08.2008 vorgestellten Ergebnisse einer von der ETH Zürich gemeinsam mit Google und IBM durchgeführten Studie: Von ca. 1,4 Milliarden PCs setzten danach 45,2 % nicht die aktuellen Versionen der jeweiligen Browser ein.

Je nach Art der Schwachstelle reicht es aus, eine entsprechend präparierte Website zu besuchen, um im schlimmsten Fall einem Angreifer die vollständige Kontrolle über das System zu überlassen. In der Tat tauchen – wie beispielsweise eine von Google am 30.07.2008 vorgestellte Studie zeigt – gerade vor Großereignissen wie den olympischen Spielen immer wieder zahlreiche manipulierte Webseiten auf, deren Besuch mit anfälligen Browsern zur Kompromittierung des Systems führen kann.

Dabei ist zu beachten, dass die Schwachstellen nicht nur die Kernkomponenten des Browsers, sondern in vielen Fällen auch Erweiterungen wie Java, Flash und Quicktime betreffen. Diese Komponenten werden gelegentlich beim Patch-Management übersehen. Eine Überprüfung der Aktualität eigener Browser-Erweiterungen und die Suche nach weiteren Schwachstellen kann bei Secunia online erfolgen. Empfehlenswert sind auch die Browserchecks vom Deutschen Sicherheitsnetz und Heise online.

Phalanx2-Rootkit

Das DFN-CERT warnte am 04.08.2008 vor einer neuen Version des bereits seit 2005 bekannten Linux-Rootkits „Phalanx“, welches in aktuellen Angriffen aus dem Internet beobachtet wurde. Phalanx2 manipuliert dabei – wie andere Rootkits auch – bestimmte Systemdateien, um sich vor Benutzer und Administrator zu verstecken. Die Infektion des Systems erfolgt überwiegend über gestohlene SSH-Schlüssel.

Linux-Administratoren sollten demnach kurzfristig überprüfen, ob ihre Systeme betroffen sind: Das DFN-CERT stellt in dem entsprechenden Security Advisory ein einfaches Shell-Skript zur Verfügung, welches nach Phalanx2-Spuren sucht.

Update legt ESX-Server lahm

Wer der Überzeugung ist, seine Sicherheit durch den Einsatz von Virtualisierung automatisch gesteigert zu haben, ist einem populären Irrglauben erlegen. Zwar kann beispielsweise durch den Einsatz von VMware ESX Server die Verfügbarkeit von Serversystemen erhöht werden. Damit handelt man sich jedoch auch zusätzliche Risiken ein. So führte ein Update für ESX in den Versionen 3.5/3.5i vom 12.08.2008 dazu, dass virtuelle Systeme auf dem ESX Server nicht mehr gestartet werden konnten. Kritisch ist dabei, dass von ESX-Fehlfunktionen unvermeidlich zahlreiche virtualisierte Serversysteme betroffen sein können. Schlimmstenfalls können komplette Serverlandschaften ausfallen.

Das Beispiel zeigt, dass bei der Einführung von Virtualisierung die damit verbundenen Risiken zu betrachten sind und – wie bei jeder kritischen Komponente einer Infrastruktur – ein besonderes Augenmerk auf den Patch-Prozess gelegt werden muss.

Eisspray gegen Krypto-Schlüssel

Dass die Inhalte des Hauptspeichers (RAM) weniger flüchtig sind als lange Zeit angenommen, weiß man aufgrund forensischer Analysen bereits seit einiger Zeit: Je nach betroffener Hardware-Betriebssystem-Kombination „überleben“ große Mengen interessanter Daten sogar das (mehrfache) Booten des Rechners.

Forscher aus Princeton, die ihre (vorab schon am 21.02.2008 unter anderem als Film in YouTube publizierten) Ergebnisse am 30.07.2008 auf dem diesjährigen USENIX Security Symposium präsentierten, gingen noch einige Schritte weiter. So fanden sie heraus, dass sich auch mehr als 60 Sekunden nach dem kompletten Ausschalten des Rechners Inhalte

aus bestimmten DRAM-Speicherchips größtenteils rekonstruieren lassen. „Behandelten“ sie die Speicherriegel eines Laptops zusätzlich mit Eisspray, bevor sie den Rechner ausschalteten, und bauten sie die gekühlten RAM-Bausteine in ein anderes Laptop ein, so konnten sie auch noch nach mehreren Minuten ohne Strom problemlos auf sämtliche RAM-Inhalte zugreifen.

Spektakulärer wird dieser Angriff durch die Tatsache, dass die Forscher zeitgleich Algorithmen und Tools zum Auffinden kryptographischer RSA- sowie AES-Schlüssel entwickelten: Mit deren Hilfe muss auf der Suche nach BitLocker-, FileVault-, dm-crypt- oder TrueCrypt-Schlüsseln nicht mehr der komplette Speicherinhalt manuell „durchstöbert“ werden. Vielleicht sollten Laptop-Nutzer zukünftig ein Wärmepflaster als Zubehör mit sich führen.

Verflüchtigung 1.3

Die künstliche Verlängerung der Flüchtigkeit von RAM-Inhalten könnte zukünftig auch bei forensischen Analysen interessant werden, da die Untersuchung des Hauptspeichers im Rahmen so genannter „Live-Analysen“ immer wichtiger wird. Längst spielt die dynamische Analyse in vielen Forensik-Projekten eine größere Rolle als die rein statische. Anzahl und Qualität der entsprechenden Tools zur Untersuchung des Hauptspeichers hielten sich bislang jedoch in Grenzen – viele Tools besaßen diesbezüglich nur rudimentäre Funktionen.

Die am 14.08.2008 erschienene neue Version der Tool-Sammlung Volatility – von ihren Entwicklern als v1.3_Beta bezeichnet – ist eine sehr mächtige, aus der Open-Source-Welt stammende kostenlose Software für Live-Analysen. Sie unterstützt Speicherdumps von Windows XP (SP2 und SP3) sowie ansatzweise Linux, kann die laufenden Prozesse anzeigen, Binaries extrahieren und offene Netzwerkverbindungen auflisten. Sie darf in keinem forensischen Werkzeugkasten fehlen.

Secorvo News

Secorvo College aktuell

Für die nächste T.I.S.P.-Schulung in der zweiten Septemberwoche (**08.–12.09.2008**) mit anschließender Zertifikats-Prüfung durch iSQI gibt es nur noch wenige freie Plätze, und auch unser „aktueller Klassiker“ mit umfangreichem Demo- und Praxisteil, das Seminar PKI – Grundlagen, Vertiefung, Realisierung am **23.–25.09. 2008**, erfreut sich großer Nachfrage – baldige Anmeldung empfohlen. Im Oktober folgen das Grundlagenseminar IT-Sicherheit heute am **07.–10.10.2008** und IT-Sicherheitsaudits in der Praxis am **28.–30.10.2008**. Termine, Programme und Online-Anmeldung unter http://www.secorvo.de/college

Symposium Wirtschaftsspionage

Im Schatten wachsender Spam- und Trojaner-Wellen nehmen gezielte Spionageattacken zu. Angesichts dieser besorgniserregenden Entwicklung führen wir gemeinsam mit dem Wirtschaftsmagazin Econo am **03.09.2008** ein eintägiges Symposium zur "Wirtschaftsspionage" durch. Ulf Tietge, Chefredakteur von Econo, wird das Symposium moderieren, für das wir zahlreiche Fachexperten wie Dr. Udo Ulfkotte und Unternehmensvertreter gewinnen konnten, die die tatsächliche Bedrohungslage analysieren und Schutzmaßnahmen vorstellen. Mit voraussichtlich über 70 Teilnehmern verspricht auch das Auditorium spannende Diskussionen. Für Schnellentschlossene gibt es noch freie Plätze (Programm, Online-Anmeldung und Anfahrtskizze).

Gut gemeint

Was ist ein "gutes" Passwort? Verbessern die verbreiteten Komplexitätsanforderungen tatsächlich die Güte gewählter Passworte? Und wie lässt sich verhindern, dass die Passworte notiert oder weitergegeben werden? Auf diese Fragen gibt eine aktuelle Untersuchung überraschende Antworten, die Thomas Maus auf dem nächsten Event der Karlsruher IT-Sicherheitsinitiative am 25.09.2008 im Schlosshotel Karlsruhe vorstellen wird. Er räumt mit einigen liebgewonnenen "Glaubenssätzen" auf und legt ein Umdenken im Umgang mit Passworten nahe. Anmeldung und weitere Informationen unter http://www.ka-it-si.de.

10 Jahre weiser

In wenigen Tagen, am 01.09.2008, wird Secorvo zehn Jahre alt. Dann werden über 550 herausfordernde Projekte, mehr als 200 veröffentlichte Aufsätze, über 70 Ausgaben der "Security News" und mehrere hundert Seminare, Symposien und Vortragsveranstaltungen hinter uns liegen. Dass wir die Chance hatten, über einen solchen - im IT-Zeitalter geradezu astronomisch langen – Zeitraum die IT-Sicherheit und den Datenschutz in Deutschland mitzugestalten, verdanken wir nicht zuletzt unseren Kunden: Deren Vertrauen in unsere Arbeit, die fruchtbare Zusammenarbeit und wohl auch die eine oder andere Empfehlung waren wesentliche Voraussetzung für diesen Erfolg.

Auch bei unseren treuen Lesern der Security News möchten wir uns bei dieser Gelegenheit bedanken. Die monatlich mehreren tausend Abrufe der News sind eine wichtige Motivation für unsere Arbeit. Und falls Sie uns schon immer einmal ein Lob aussprechen wollten – anlässlich unseres runden Geburtstags würde uns das besonders freuen.

Veranstaltungshinweise

Auszug aus http://www.veranstaltungen-it-sicherheit.de

September 2008	
03.09.	Symposium Wirtschaftsspionage (Secorvo, Ettlingen)
07.-10.09.	OSS 2008 – 1st Workshop on Open Source Software for Computer and Network Forensics (IFIP, Milano/IT)
08.-12.09.	T.I.S.P.-Schulung (Secorvo College)
23.-26.09.	PKI – Grundlagen, Vertiefung, Realisierung (Secorvo College)
23.-25.09.	IMF 2008 – 4th International Conference on IT-Incident Management & IT-Forensics (GI, Mannheim)
Oktober 2008	
07.-10.10.	IT-Sicherheit heute (Secorvo College)
28.-30.10.	IT-Sicherheitsaudits in der Praxis (Secorvo College)
November 2008	
04.-05.11.	Security Awareness - Methoden, Konzepte, Best Practice (Secorvo College)
11.-13.11.	Forensik - Verfahren, Tools, Praxis (Secorvo College)

Fundsache

Die Kryptoanalyse mathematischer Algorithmen ist seit vielen Jahrhunderten eine anspruchsvolle Wissenschaft. Zahlreiche Fachbücher existieren zu diesem Thema; nicht immer sind die Erläuterungen aber für Einsteiger verständlich. Der Google-Mitarbeiter Mark Chu-Carroll hat am 15.08.2008 in seinem Blog eine sehr informative Einführung in die Kryptoanalyse „zum Nachmachen" gegeben – auch die Kommentare sind lesenswert.

Impressum

http://www.secorvo-security-news.de

ISSN 1613-4311

Redaktion: Dirk Fox, Stefan Gora, Stefan Kelm

Herausgeber (V. i. S. d. P.): Dirk Fox
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses:
security-news@secorvo.de
(Subject: „subscribe security news")

Wir freuen uns über Ihr Feedback an
redaktion-security-news@secorvo.de

secorvo
security consulting

Secorvo Security News

September 2008

Editorial: Verhältnisunmäßig

Große Erregung: Millionen Kontendaten, für kleines Geld zu erwerben, bieten fette Beute für Betrüger, die Banken glaubhaft versichern, im Besitz von Einzugsermächtigungen zu sein. Verbraucherschützer trommeln, die Republik ist empört, und der Bundesinnenminister gipfelt.

Die richtige Aufregung, aber zum falschen Anlass. Seit 1998 wertet Google täglich Milliarden Suchanfragen zur Erstellung und Verfeinerung von Abfrageprofilen aus. Zähneknirschend hat Google am 08.09.2008 auf Druck der Artikel-29-Gruppe den europäischen Datenschutzbeauftragten angekündigt, „damit zu beginnen", die IP-Adressen in den Such-Logs schon (sic!) nach neun Monaten zu anonymisieren. Sechs Tage zuvor hatte Google seinen neuen Browser Chrome publiziert. Welch Koinzidenz. Millionenfach heruntergeladen, erlaubt Chrome die Verknüpfung von Suchanfragen mit Webseitenaufrufen – und einer eindeutigen Browser-ID. Abgleiche der Suchprofile mit den Webseiten von Social Networks, Personensuchmaschinen wie 123people oder yasni, den Adressangaben in Telefonbüchern oder Nachbarbeschimpfungen liefern Google (und z.T. auch dessen Nutzern) von immer mehr Menschen ein Persönlichkeitsprofil. Von da zum Großen Bruder ist es nur noch einen klitzekleiner Klick. Wer braucht da noch die sechsmonatige Vorratsdatenspeicherung?

Immerhin regt sich inzwischen etwas im Innenministerium. Sogar in die seit sieben Jahren überfällige Verabschiedung eines Datenschutz-Audit-Gesetzes, an die kein Datenschützer mehr zu Glauben wagte, kommt Bewegung. Allerdings lassen einige der Gipfelergebnisse eher operative Hektik befürchten: Durch die Abschaffung des Listenprivilegs würde keine einzige Kontonummer gerettet, und ein Kopplungsverbot wiese Google nicht in die Schranken.

„Wer weiß, wie Gesetze und Würste zu Stande kommen, kann nachts nicht mehr gut schlafen", soll Otto von Bismarck gesagt haben. Den meisten Metzgern würde er heute damit Unrecht tun.

Inhalt

Security News

WASC Studie

Am 08.09.2008 hat das Web Appliction Security Consortium (WASC) die Ergebnisse des Projekts „Web Application Security Statistics 2007" veröffentlicht. Im Rahmen dieser Studie wurden zum besseren Verständnis der Sicherheitslage bei Web-Anwendungen über 32.000 Sites automatisiert und manuell untersucht. Die im Detail vorgestellten Ergebnisse sind aufschlussreich und erschreckend zugleich: Wenn auch nur knapp über 7% der untersuchten Anwendungen automatisiert kompromittiert werden konnten, wurden in über 96% der Anwendungen bei manueller Suche schwerwiegende Schwachstellen gefunden. Insbesondere handelte es sich um Anfälligkeiten für Cross-Site-Scripting, Information Leakage, SQL-Injection und Predictable Resource Location.

Als Basis diente die WASC Threat Classification 1.0 aus dem Jahr 2005. Trotz der etwas betagteren Grundlage bietet die Studie eine umfassende Analyse der benutzten Methoden und erzielten Ergebnisse. In diesem Zusammenhang triff es sich gut, dass am 15.09.2008 der Aufruf zur Mitarbeit an der Weiterentwicklung zur WASC Threat Classification 2.0 erfolgte. Allen an Web-Sicherheit Interessierten legen wir die Beobachtung dieser Entwicklung sehr ans Herz.

Nmap auswerten

Am 07.09.2008 ist der Netzwerkscanner Nmap in Version 4.75 erschienen. Darin wurde das GUI Zenmap um die Visualisierungskomponente Radialnet erweitert. Zwei sehr sinnvolle Funktionen – Datenaggregation mehrerer Scans und eine Netztopologiedarstellung – stehen nun zur Verfügung, sofern die Scan-Ergebnisse im XML-Format vorliegen.

Dies vereinfacht die Analyse der Scanergebnisse erheblich, da zeitlich auseinanderliegende Scans in einer Auswertung darstellbar sind – der Praktiker weiß: Nicht immer sind alle Hosts online oder dürfen im selben Arbeitsablauf gescannt werden. Erfreulicherweise funktioniert die Aggregation auch mit älteren XML-Dateien des 4.60-Releases. Die Topologie des Netzwerks ist konzentrisch und mit relativer Hopdistanz darstellbar, inklusive Ergebnisdetails für gescannte IPs. Ein übersichtlicher Netzplan als Nebenprodukt eines Audits ist ein erheblicher Mehrwert. Ein Wermutstropfen bleibt: Für umfangreiche IP-Ranges braucht man viel CPU-Zeit – und scharfe Augen.

Rootkit für Jedermann

Am 03.09.2008 wurde das voll funktionsfähige Open Source Rootkit „Debug Register" (DR) in der Version 0.1 für Linux-Kernels 2.6.x (Intel-IA32-Architekturen) vom Penetrationstest-Werkzeughersteller Immunity Inc. zum Download veröffentlicht. Seine Funktionen umfassen die Unterstützung für versteckte Prozesse, Netzwerksockets, Daten sowie eine Backdoor.

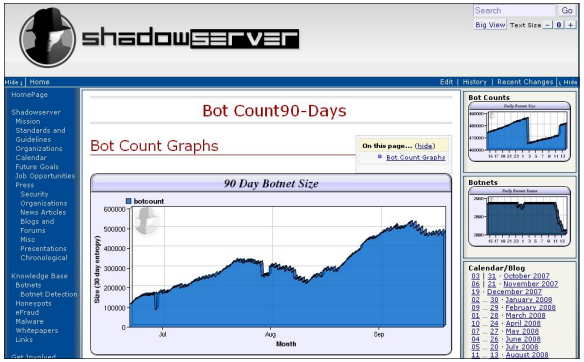
Das Rootkit arbeitet wie ein Kernel-Debugger und nutzt vorhandene System-Interrupts der Intel-CPUs – eine Technik, die bisher von Malware kaum eingesetzt wurde, da dafür ein tiefes Systemverständnis erforderlich ist. Mit einem Entwicklungsaufwand von ca. zwei Wochen lässt sich der Code um eine Tarnung auf Kernel-Ebene erweitern.

Damit wurde die Entwicklung leistungsfähiger Malware im Linux-Umfeld erheblich beschleunigt. Ohne einen wirksamen Integritätsschutz der Systemumgebung ist gegen derartige Low-Level-Angriffe kein Kraut gewachsen.

Botnetz-Wachstum

Die 2004 gegründete Shadowserver Foundation hat sich zur Aufgabe gemacht, die „dunklen Seiten des Internet" zu beleuchten. Von Sicherheitsspezialisten werden die Entwicklungen bei Viren und Malware sowie von Botnetzen beobachtet; Ergebnisse und weitere Informationen werden auf den Webseiten der Initiative veröffentlicht.

Dabei wurde in den vergangenen drei Monaten ein sprunghaftes Wachstum von Botnetzen beobachtet: Die geschätzte Anzahl der übernommenen Systeme hat sich fast vervierfacht. Ursache hierfür dürften unter anderem Malware-Mailings anlässlich der Olympiade sein. Auch wurden PCs verstärkt über kompromittierte Webserver infiziert.



Die Entwicklung zeigt, dass es weiterer technischer und organisatorischer Maßnahmen bedarf, um Client-Systeme adäquat zu schützen. Nutzern empfehlen wir die Beachtung entsprechender Warnungen, beispielsweise unter www.bsi-fuer-buerger.de.

Endlich DNSSEC?

Die Schwächen des Internet Domain Name Systems (DNS), die bei den unlängst veröffentlichten Cache Poisoning Attacken (siehe SSN 07/08) zu Tage traten, kommen nicht überraschend. Bereits im Januar 1997 wurde in RFC 2065 die erste Version der DNS Security Extensions (DNSSEC) veröffentlicht. Nach zwei Überarbeitungen ist DNSSEC seit März 2005 in den RFCs 4033 ff. spezifiziert und in verbreiteter DNS-Software, z. B. BIND, integriert – kann also nach Internet-Zeitmaßstäben als ausgereift gelten.

DNSSEC nutzt elektronische Signaturen zur Sicherung der erteilten Auskünfte. Die dabei benötigte PKI wird jedoch nicht wie üblich über X.509-Zertifikate realisiert; statt dessen erteilen Nameserver direkt Auskunft über die Public Keys der Nameserver darunter liegender Ebenen. Hierin liegt auch einer der Gründe, dass DNSSEC trotz langer Vorlaufzeit noch nicht global eingesetzt wird: Genau so umstritten wie die Kontrolle über die Root-Nameserver ist auch die politische Frage, wer deren Schlüsselpaar als „Trust Anchor" des Internet kontrollieren soll.

Mit Erlass vom 22.08.2008 ordnete die US-Regierung – kaum zufällig zeitgleich mit den jüngsten DNS-Attacken – für die von ihr kontrollierte Government Top-Level Domain („gov") die flächendeckende Einführung von DNSSEC bis Ende 2009 an. Die einschlägigen Umsetzungsempfehlungen der NIST Special Publication 800-81 sind für jeden DNS-Verantwortlichen einen Blick wert.

Ein Multiplikator-Effekt könnte sich einstellen, wenn Service-Provider, die für einzelne Behörden deren .gov-Domains hosten, ihre Insfrastruktur fit für DNSSEC machen müssen und diesen Zusatz-Dienst dann auch anderen Kunden anbieten.

Datenschutz-Bußen

Weder die öffentliche Zerknirschung noch der Rückgriff auf den ehemaligen Bundesdatenschutzbeauftragten Jakob haben Lidl geholfen: Am 11.09.2008 verkündeten die Datenschutzaufsichtsbehörden die Verhängung von Bußgeldern in einer Gesamthöhe von knapp 1,5 Mio. Euro, nachdem Lidl seine Mitarbeiter in persönlichkeitsverletzender Weise hatte ausspionieren lassen. Eigenwillige Interpretationen von Arbeitnehmerrechten hatten bereits 2004 zur Verleihung des BigBrotherAward geführt.

Dass es sich beim persönlichkeitsverletzenden Einsatz von Videoüberwachung nicht um ein Kavaliersdelikt handelt, wird auch durch das am 15.09.2008 von der nordrhein-westfälischen Aufsichtsbehörde gegen den Fleischverarbeiter Tönnies verhängte Bußgeld in Höhe von 80.000 Euro bekräftigt. Zur Diebstahlsvorbeugung wurden die Beschäftigten mit über 200 Kameras unter anderem auch in Umkleidekabinen und Sozialräumen überwacht.

Eine gesetzeskonforme Gestaltung der Verarbeitung personenbezogener Daten gebietet inzwischen auch die ökonomische Vernunft. Die Zeiten, in denen sich Datenschutzverstöße aussitzen ließen, sind vorbei.

Secorvo News

Secorvo College aktuell

Pünktlich zu den in Karlsruhe gelegentlich auch im Spätsommer noch südländischen Temperaturen lockt Secorvo College nun mit klimatisierten Räumen. Das scheint sich schnell herumgesprochen zu haben, denn mehrere Seminare waren schon kurz nach dem Ende der Urlaubszeit ausgebucht.

Noch freie Plätze gibt es für die Seminare IT-Sicherheit heute (**07.–10.10.**), IT-Sicherheitsaudits (**28.–30.10.**), Security Awareness (**04.–05.11.**) und das T.I.S.P.-Seminar (**24.–28.11.**).

Programm und Online-Anmeldung unter http://www.secorvo.de/college

Für das Seminar Forensik, das sich ganz besonderer Nachfrage erfreut, haben wir eine Warteliste eingerichtet. Voraussichtlich im Januar 2009 wird es einen zusätzlichen Termin geben. Bitte wenden Sie sich bei Interesse an college@secorvo.de.

Gut gemeint

„Das Gegenteil von gut ist nicht böse, sondern gut gemeint." Das gilt leider auch für verbreitete Passwort-Policies, wie Thomas Maus in seinem Vortrag im Rahmen der Karlsruher IT-Sicherheitsinitiative (KA-IT-Si) am 25.09.2008 (18 Uhr im Schlosshotel Karlsruhe) zeigen wird. Dabei räumt er mit vielen lieb gewonnenen und, wie das obige Zitat von Gottfried Benn, gerne kopierten „Wahrheiten" auf. Im Anschluss an den Vortrag gibt es, wie gewohnt, Gelegenheit zum Buffet-Networking. Um Anmeldung wird gebeten.

Jubiläums-Nachlese

Für die zahlreichen Glückwünsche, die uns zu unserem 10jährigen Firmenjubiläum erreicht haben, bedanken wir uns auch an dieser Stelle sehr herzlich. Auch die vielen „Geburtstagslob"-E-Mails zu unseren News haben uns sehr gefreut – wir bleiben am Ball, versprochen. Mit den Vorbereitungen für den 20sten Jahrestag haben wir auch schon begonnen.

Veranstaltungshinweise

Auszug aus http://www.veranstaltungen-it-sicherheit.de

September 2008	
25.09.	Das Gegenteil von gut ist - gut gemeint (KA-IT-Si)
Oktober 2008	
07.-10.10.	IT-Sicherheit heute (Secorvo College)
07.-09.10.	ISSE (TeleTrust), Madrid/ES
27.-30.10.	Hack-in-the-Box 2008, Kuala Lumpur/MY
28.-30.10.	IT-Sicherheitsaudits in der Praxis (Secorvo College)
November 2008	
04.-05.11.	Security Awareness - Methoden, Konzepte, Best Practice (Secorvo College)
11.-13.11.	Forensik – Verfahren, Tools, Praxis (Secorvo College)
18.-21.11.	Information Security Management (Secorvo College)
24.-28.11.	T.I.S.P.-Schulung (Secorvo College)
Dezember 2008	
02.-04.12.	Sichere Softwareentwicklung (Secorvo College)

Fundsache

Bei der Betätigung des „Home Buttons“ eines iPhones schrumpft die aktuell offene Anwendung und blendet sich aus. Dieser optische Effekt wird im iPhone durch das Erstellen von Bildschirmfotos realisiert – SubSeven lässt grüßen. Das iPhone löscht ältere Fotos zwar, aber bei einer forensischen Untersuchung des iPhones treten diese Spuren offenbar wieder hervor. Ein Feature für die Strafverfolgung – oder ein Westentaschenspion?

Impressum

http://www.secorvo-security-news.de

ISSN 1613-4311

Redaktion: Dirk Fox, Stefan Gora, Kai Jendrian, Karin Schuler, Hans-Joachim Knobloch, Jochen Schlichting

Herausgeber (V. i. S. d. P.): Dirk Fox
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses:
security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an
redaktion-security-news@secorvo.de

secorvo
security consulting

Secorvo Security News

Oktober 2008

Editorial: One man – no vote?

Wählen mit Computerhilfe – der Traum aller Wahlhelfer, die unter Zeitdruck tausende Stimmzettel auszählen müssen. Einfach bestechend: Per Mausklick lassen sich Auszählung und Wahlvorgang beschleunigen und Zählfehler ausschließen.

Elektronische Wahlen sind nichts Neues in Deutschland. Die Gesellschaft für Informatik wählt ihr Präsidium seit 2004 über das Internet, an Universitäten wird die Selbstverwaltung mit Computerhilfe bestimmt und in mehreren Bundesländern werden Wahlcomputer bei Kommunal-, Landtags- und Bundestagswahlen eingesetzt. Am 24.10.2008 erhielt Bingo Voting, ein an der Universität Karlsruhe entwickeltes Verfahren mit der Möglichkeit zur Prüfung der korrekten Zählung der eigenen Stimme, den Deutschen Sicherheitspreis 2008.

Tatsächlich ist E-Voting nicht so einfach, wie es scheint. Denn aus der Perspektive des Wählers ist ein Wahlcomputer eine Black Box, der er bei Stimmabgabe blind vertrauen muss. Nicht immer ist dieses Vertrauen berechtigt. So wird in Deutschland der Nedap-Wahlcomputer eingesetzt, ein Gerät, dessen Version ES3B der Chaos Computer Club (CCC) 2006 analysiert hat – mit bitteren Ergebnissen: Der Manipulationsschutz beruht auf simplen, leicht fälschbaren Papiersiegeln, das Master-Passwort war mit „GEHEIM" vorbelegt, und durch einen Firmwaretausch ließ sich der Wahlcomputer in einen Schachcomputer verwandeln (siehe SSN 10/2006). In Brandenburg stellten Wahlbeobachter des CCC am 28.09.2008 – wie zuvor in Hessen – erhebliche Mängel beim Umgang mit den Wahlcomputern fest: Fehlende Siegel, unbeaufsichtigte Lagerung, Fehlbedienung und unerklärliche Zähldifferenzen.

Manipulierbare Wahlcomputer wären eine gefährliche Waffe in den Händen einer Partei oder Regierung. Stimmzettel lassen sich durch Unabhängige nachzählen – Computerdaten nicht. Das wurde auch in der öffentlichen Anhörung vor dem Bundesverfassungsgericht am 28.10.2008 deutlich. Bleibt zu hoffen, dass Papier und Bleistift noch eine Chance haben – wenigstens dann, wenn der Souverän wählt.

Inhalt

secorvo
security consulting

Security News

Clickjacking

Auf der diesjährigen amerikanischen OWASP-Konferenz sorgte das Zurückziehen eines Vortrags zum Thema „Clickjacking“ durch die Autoren Robert „RSnake“ Hansen und Jeremiah Grossman für einiges Aufsehen. Inzwischen sind durch einen Blog-Eintrag Robert Hansens vom 07.10.2008 sowie die Veröffentlichung eines Proof of Concept und eines Videos erste Details zu der architektonisch bedingten Schwachstelle bekannt. Darin werden verschiedene Ausprägungen vorgestellt.

Clickjacking wird das Platzieren eines „unsichtbaren“ Click-Buttons auf einer Webseite genannt, auf den der Nutzer klickt, während er vermeintlich einen darunter liegenden Link auswählt. Bis zur Beseitigung dieser Browserschwachstelle bietet das – auch in anderem Kontext sehr nützliche – Firefox Add-On „NoScript“ mit „ClearClick“ einen gewissen Schutz.

Forensische Spirale 2.0

Seit vielen Jahren schon gehört die Live-CD Helix in den virtuellen Werkzeugkasten jeder Forensikerin. Helix ist eine der wenigen umfangreichen Tool-Sammlungen, die sowohl unter Windows als auch unter Linux zu verwenden sind – sie war allerdings schon etwas in die Jahre gekommen.

Am 15.09.2008 wurde endlich die von vielen herbei gesehnte Helix Version 2.0 veröffentlicht. Wir haben die neue Version in unserem forensischen Labor ausgiebig getestet. Ergebnis: Das Warten hat sich gelohnt. Zunächst wurden die einzelnen Tools auf den neuesten Stand gebracht bzw. um neue Software ergänzt. Die größte Änderung ist jedoch der Umstieg der Boot-Partition auf Ubuntu, was u. a. die Unterstützung neuer Hardware spürbar verbessert. Helix 2.0 ist und bleibt damit eine interessante Ergänzung oder sogar Alternative zu kommerziellen forensischen Tools. Wir werden Helix 2.0 bereits im kommenden Forensik-Seminar berücksichtigen.

Neue Hash-Funktionen

SHA, der Secure Hash Standard, war die erste standardisierte Hashfunktion, 1994 vom US-amerikanischen NIST veröffentlicht. Am 01.08.2002 legte das NIST mit einer erweiterten Spezifikation nach, die vier Varianten der nun SHA-2 genannten Algorithmenfamilie mit unterschiedlich langen Hashwerten umfasste (FIPS PUB 180-2). 2004 wurde die Spezifikation um die Variante SHA-224 ergänzt; eine Endfassung des Standards erschien am 17.10.2008 (FIPS PUB 180-3).

Doch die Tage des in die Jahre gekommenen SHA-2 sind gezählt. Da für einen Nachfolger keine geeigneten alternativen Verfahren in Sicht waren, schrieb das NIST am 02.11.2007 – wie beim AES – einen Wettbewerb für SHA-3 aus. Wenige Tag vor der Einreichungsfrist (31.10.2008) waren schon über 30 Verfahren beim NIST eingegangen. Ein sehr aussichtsreicher Kandidat ist der Skein getaufte Algorithmus einer Kryptographengruppe um Bruce Schneier. Auch ein „Veteran“ ist dabei: Ron Rivest, einer der Väter des RSA-Verfahrens, hat MD6 ins Rennen geschickt.

Virenschutz für VMs

Vom Virenschutz-Anbieter McAfee wurden am 17.09.2008 Lösungen zum Scannen von virtuellen Maschinen vom Virtualisierungs-Host aus (VMware ESX) vorgestellt. Auf den ersten Blick ein vorteilhafter Ansatz: Virtuelle Maschinen werden, auch wenn sie nicht verwendet werden, zentral überprüft, und bei Bedarf wird sogar der auf den Gastsystemen installierte Virenschutz aktualisiert.

Aber Vorsicht: Jedes Gastsystem sollte – wie bei „echten“ physikalischen Servern – über einen installierten und regelmäßig aktualisierten Virenschutz verfügen. Einen Mehrwert bietet die neue Produktserie nur dann, wenn die Systeme gerade ausgeschaltet sind. Auch besteht die Gefahr, sich durch die zusätzliche Software auf dem Hostsystem Angriffsmöglichkeiten und Sicherheitsprobleme einzuhandeln. Denn in den Listen von Produkten mit sicherheitskritischen Fehlern fanden sich in den vergangenen Jahren zahlreiche Hersteller und Produkte von Sicherheitssoftware.

Unsere Empfehlung lautet daher: Keep it simple. ESX-Systeme sollten ohne Verwässerung der Sicherheitsfunktionen wie guter schottischer Whisky genossen werden: pur – und ohne Eis.

Surf-CD vom BSI

Am 08.08.2008 wurde vom BSI eine auf Knoppix basierende „Surf-CD“ vorgestellt. Die Idee dahinter ist, durch Booten von CD ein sauberes System zu erhalten und damit bspw. sicheres Online-Banking zu ermöglichen. Dazu wurde das von CD zu startende System durch mehrere Maßnahmen gehärtet und der verwendete Browser „Iceweasel“, die Debian-Variante von Firefox, durch Sicherheits-Plugins aufgepeppt. Im Vergleich zu anderen Boot-CDs überzeugt unter anderem, dass ein schreibender Zugriff auf weitere Datenträger, beispielsweise auf interne oder externe Festplatten des Systems, kernelseitig unterbunden wird.

Eine gute Lösung für Anwender, die ihr System beim Surfen vor eingefangener Schadsoftware

schützen möchten – oder dem vom Filius zum Spielen genutzten System nicht mehr ihre PINs und TANs anvertrauen mögen.

OWASP Appsec 2008

Am 24.-25.09.2008 fand die OWASP NYC Appsec 2008 Conference im Big Apple statt. Das wachsende Interesse an Applikationssicherheit wurde durch die ansehnliche Zahl von über 850 Teilnehmern eindrucksvoll verdeutlicht. Die an der einen oder anderen Stelle dadurch verursachten Reibungsverluste wurden durch die engagierte Konferenzorganisation überkompensiert.

Fachlich hatte die Tagung einige Highlights zu bieten. Hervorzuheben sind die Vorträge von Gunter Ollmann zum Thema „Multidisciplinary Bank Attacks", Ausflüge in die Praxis von Angriffen wie „Get Rich or Die Trying – Making Money on The Web, The Black Hat Way" von Tom Brennan, Jeremiah Grossman und Trey Ford. Für Interessierte, die nicht an der Konferenz teilnehmen konnten oder verpasste Parallelvorträge ansehen möchten, stehen die Videos der Vorträge online bereit.

Die vorgestellten theoretischen und praktischen Arbeiten sind für die Beschäftigung mit verschiedenen Aspekten der Applikationssicherheit wertvoll. Daher sollte man den Termin der OWASP Germany 2008 Conference am 25.11.2008 in Frankfurt vormerken.

Mifare-Exploit online

Jetzt ist es passiert: Am 27.10.2008 hat ein Hacker unter dem Pseudonym 'Bla' eine C-Implementierung des von der Radboud Universiteit Nijmegen auf der europäischen Sicherheitskonferenz Esorics am 06.-08.10.2008 publizierten Angriffs auf Mifare Classic mit dem Titel „crapto1" auf der Open Source Platform Google Code veröffentlicht. Zwar fehlt zu einer „Plug-and-Play"-Attacke noch die Software für Proxmark oder den OpenRFID Sniffer. Für deren Implementierung sind jedoch keine kryptologischen Kenntnisse erforderlich; die öffentliche Bereitstellung ist daher nur eine Frage der Zeit.

Jetzt hilft kein Abwiegeln mehr: Das Clonen und Manipulieren von Mifare-basierten Chipkarten wird in Kürze ein Kinderspiel sein. Wer Mifare Classic einsetzt, sollte sich daher baldigst geeignete Migrationsstrategien einfallen lassen, um nicht gegen Sorgfaltspflichten zu verstoßen.

BSI meets ISACA

Der bereits am 01.09.2008 veröffentlichte „Leitfaden für die IS-Revision auf Basis von IT-Grundschutz" bildet die Grundlage für die Durchführung von IS-Revisionen in Bundesbehörden gemäß des UP Bund. Das konzeptionell klar strukturierte, 37-seitige Dokument enthält neben den konkreten Durchführungsschritten auch eine Aufwandsschätzung über 30 bis 100 Personentage für die so genannte Querschnittsprüfung. Daraus wird ersichtlich, dass Initial- und Betriebsaufwand für das Thema Informationssicherheit deutlich höher sind als das, was viele Behörden operativ investieren. Als Fachqualifikation für die Befähigung zur IS-Revision wird allgemein auf einen „Nachweis der Qualifikation durch Zertifikate" verwiesen. Eine Chance für den IT-Grundschutz?

Im Oktober 2008 hat das ISACA Germany Chapter den – nur in Papierform erhältlichen – „Leitfaden zur Durchführung eines Quality Assurance Reviews der Internen IT-Revision (QAR-IT)" veröffentlicht. Der zehnseitige Prüfungskatalog ist eindeutig und sehr aussagefähig und wird durch eine vollständige Liste aller Prüfungsstandards abgerundet. Er ist zudem so universal einsetzbar, dass damit auch eine QAR für eine IS-Revision durchgeführt werden kann. In Kombination mit dem Leitfaden des BSI lässt sich damit auch die Frage nach der „Kontrolle des Kontrolleurs" beantworten.

Secorvo News

Secorvo College aktuell

Für Schnellentschlossene bietet Secorvo College 2008 noch zwei Weiterbildungschancen:

- Information Security Management von A(udit) bis Z(erzifizierung) am **18.–21.11.2008** sowie eine
- T.I.S.P.-Schulung am **24.–28.11.2008** mit anschließender Prüfung.

Die Termine der Seminare 2009 stehen inzwischen ebenfalls fest – eine praktische Übersicht bietet der ganzjährige College-Kalender.

Detaillierte Seminarprogramme und die Möglichkeit zur Online-Anmeldung (auch schon für 2009) finden Sie unter http://www.secorvo.de/college.

Original oder Fälschung?

Seit fast 20 Jahren prägt ein Karlsruher Unternehmen, die WIBU-Systems AG, die weltweite Entwicklung des „Digital Rights Managements" zum Schutz digitaler Produkte – Software, Dokumente, Medien. Auf dem letzten diesjährigen Event der Karlsruher IT-Sicherheitsinitiative (KA-IT-Si) am 04.12.2008 wird Rüdiger Kügler spannende Einblicke in die rasante Entwicklung der DRM-Technologie geben – und zeigen, was uns hinsichtlich des Schutzes digitaler Güter in den kommenden Jahren erwartet.

Veranstaltungshinweise

Auszug aus http://www.veranstaltungen-it-sicherheit.de

November 2008	
04.-05.11.	Praxistage Datenschutz (BvD, Stuttgart)
11.-13.11.	Forensik (Secorvo College)
18.-21.11.	Information Security Management (Secorvo College)
24.-28.11.	T.I.S.P - Schulung (Secorvo College)
25.11.	OWASP Germany 2008 Conference (www.owasp.org, Frankfurt)
29.-30.11.	ruxcon 2008 (ruxcon.org, Sydney/AU)
Dezember 2008	
04.12.	„Das Original ist die beste Kopie“ (KA-IT-Si, Karlsruhe)
27.-30.12.	25th Chaos Communication Congress (CCC, Berlin)
Januar 2009	
20.-22.01.	Omnicard 2009 (inTIME, Berlin)

Fundsache

Am 29.09.2008 hat das US-amerikanische NIST in der Reihe Special Publication einen 80seitigen „Technical Guide to Information Security Testing and Assessment“ (NIST Special Publication 800-115) veröffentlicht, das eine sehr hilfreiche und praktisch-konkrete Handreichung zur Durchführung von Information Security Audits darstellt. Alle wesentlichen Risiken einer Netzwerkinfrastruktur werden betrachtet und eine systematische Vorgehensweise für deren Analyse vorgeschlagen. Abgerundet wird das instruktive Dokument durch eine aktuelle Liste frei verfügbarer Tools und Informationsquellen über bekannte Schwächen.

Impressum

http://www.secorvo-security-news.de

ISSN 1613-4311

Redaktion: Dirk Fox, Alexander Göbel, Stefan Gora, Kai Jendrian, Stefan Kelm, Jochen Schlichting

Herausgeber (V. i. S. d. P.): Dirk Fox
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses:
security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an
redaktion-security-news@secorvo.de

secorvo
security consulting

Secorvo Security News

November 2008

Editorial: Geschichtsvergessen

Das aktuelle Politbarometer der Mannheimer Forschungsgruppe Wahlen vom 21.11. 2008 enthält die erste repräsentative Befragung zur geplanten Ermächtigung des BKA zu Online-Durchsuchungen. Das ernüchternde Ergebnis: 57% der Deutschen halten die Befugnis für grundsätzlich richtig, 39% sprachen sich dagegen aus.

Ist das stereotype „ceterum censeo" des BKA-Präsidenten, eine verbreitete „Ich-hab-nichts-zu-verbergen"-Mentalität oder die mediale Beschwörung der terroristischen Bedrohung (zum Vergleich: 2007 starben in Deutschland 340 Menschen durch Mord, 600 bei Brandkatastrophen und knapp 5.000 bei Verkehrsunfällen – und niemand bei einem Terroranschlag) für dieses Ergebnis verantwortlich?

Vor 40 Jahren, im Sommer 1968, trieben die als „Ermächtigungsgesetz" geziehenen Notstandsgesetze der Großen Koalition Jugendliche und Studenten zu Tausenden auf die Straßen. Die Ermächtigung der Nachrichtendienste im G-10-Gesetz zu Eingriffen in das Post- und Fernmeldegeheimnis – unter strenger parlamentarischer Kontrolle durch die G-10-Kommission – war eines der zentralen politischen Reibungspunkte der Außerparlamentarischen Opposition, aus deren Trümmern zwei Jahre später die RAF hervorging.

Heute bleibt Deutschland angesichts der fortschreitenden Aushöhlung des Fernmeldegeheimnisses gelassen. Während die Liste der Katalogstraftaten in § 100 StPO, die Abhörmaßnahmen rechtfertigen, schrittweise ausgeweitet wurde und die Zahl der Abhöranordnungen von 1985 (1.400) bis 2007 (44.280) auf das 30-fache anstieg (vgl. SSN 06/2006), wirkt selbst die Aufregung über die Auswertung der Verbindungsdaten von Journalisten durch die Deutsche Telekom angestrengt. Bei der verfassungswidrigen Durchsuchung der Redaktionsräume des „Spiegel" im Jahr 1962 hatte es noch zu einer Entscheidung des BVerfG, dem Spiegel-Urteil vom 05.08.1966 gereicht.

Wie formulierte Alexis de Tocqueville 1835 doch so zutreffend: „Die schlimmsten Feinde der Freiheit – sind die glücklichen Sklaven."

Inhalt

secorvo
security consulting

Security News

Kryptographie bleibt schwierig

Mitglieder des Google Security Teams meldeten am 11.08.2008 in ihrem Blog eine Lösung für das Problem, wie Anwendungsentwickler Kryptoverfahren einfach und sicher einsetzen können: das bei Google gehostete Open-Source Crypto-Toolkit Keyczar. Zielpublikum für die in Java und Phyton vorliegende Keyczar-Implementierung sind primär Web-Entwickler – und zwar solche, die den Keyczar-Autoren zufolge schlimmstenfalls Schlüssel fest im Quellcode ihrer Anwendung hinterlegen würden.

Für Entwickler der letztgenannten Ignoranzklasse mag das Toolkit tatsächlich eine Hilfe sein. Ansonsten aber zeigt ein Blick in das Designdokument, dass Keyczar keine Konkurrenz für die direkte Nutzung von OpenSSL & Co. ist und hinter den eigenen Ansprüchen zurück bleibt. Denn nicht nur für die Bundesnetzagentur zählen SHA-1 und 1024 Bit DSA schon lange nicht mehr zu den „safe default algorithms and key lengths".

Schlimmer wiegt, dass Keyczar zwar optional geheime Schlüssel auch verschlüsselt ablegt, dafür aber einen unverschlüsselten Masterkey im eigenen Format braucht. Die Gefahr ist groß, dass Web-Entwickler die Schlüssel zwar nicht mehr im Quellcode „verstecken", dafür aber den Masterkey offen als Datei ablegen - und sich dabei sicher wähnen.

Das Zweitschlimmste nach dem Irrtum, Sicherheitsverfahren wären einfach selbst zu entwickeln, sind wohl Systeme, die vorgeben, dem Entwickler die nötigen Kenntnisse zu deren Einsatz zu ersparen.

Neue Schlüssel – gute Schlüssel?

Die am 07.11.2008 veröffentlichte NIST Special Publication 800-108 zum Thema „Key Derivation" zeigt, dass ein erläuternder Standard anstelle eines Black-Box-Toolkits wie Keyczar die Anwendung von Kryptoverfahren vielleicht nachhaltiger erleichtern kann.

Auf 20 Seiten wird dargestellt, wie sich aus einem vorhandenen Schlüssel viele (z. B. für automatisierte Schlüsselwechsel) ableiten lassen, wird hingewiesen, worauf beim Einsatz dieser Verfahren zu achten ist, und wird motiviert, warum manch scheinbar unnützer „Schnörkel" dabei hilfreich ist.

Das Dokument legen wir jedem Entwickler dringend ans Herz, der eine sichere Schlüsselverwaltung entwerfen will.

WPA-Erbsünde rächt sich

Als im Jahr 2001 nach erfolgreichen Angriffen auf das Wired Equivalent Privacy (WEP) Protokoll dringend Abhilfe für die Sicherung von WLANs gesucht wurde, war der erste Wurf für das neue Wifi Protected Access (WPA) Verfahren gar nicht so neu: Das Temporal Key Integrity Protocol (TKIP) des Standards IEEE 802.11i setzt auf der WEP-Verschlüsselung auf, ergänzt um weitere Sicherheitsmechanismen und regelmäßige Schlüsselwechsel. Durch diesen Trick wurde es möglich, allein per Firmware-Update aus vorhandenen, unsicheren WEP-Produkten neue WPA-Produkte zu machen.

Am 08.11.2008 veröffentlichten Martin Beck und Erik Tews, Forscher der Unis Dresden und Darmstadt (woher 2007 schon die bis heute schnellste WEP-Attacke stammt, vgl. SSN 04/07), einen Weg, um trotz der zusätzlichen Vorkehrungen in TKIP über eine ererbte WEP-Schwachstelle einen Teil des RC4-Schlüsselstroms von WEP bzw. TKIP zu ermitteln. Diese Information erlaubt es, einige wenige Datenpakete vom Access Point an WLAN-Clients zu fälschen, beispielsweise zum gezielten Umleiten von Verbindungen.

Wie vor zehn Jahren bei Daniel Bleichenbachers Angriff auf SSL mit RSA hilft hier wieder das Entgegenkommen der Protokolldesigner: Erst die Rückmeldung, die verrät, an welcher Stelle Entschlüsseln und Prüfen eingeschleuster Daten fehlschlagen, zeigt dem Angreifer, wie weit er vorgedrungen ist. Der neue alte Angriff ist nicht so fatal wie die WEP-Attacken und eröffnet keine völlig neuen Angriffswege gegen WPA oder den Nachfolger WPA2. Dennoch sollte man der AES-CCMP Verschlüsselung von WPA2 den Vorzug vor TKIP geben – oder zumindest die TKIP-Schlüsselwechsel auf unter 120 s beschleunigen.

Sicherere Software

Die Entwicklung sicherer Software liegt im Trend: Endlich wird das Problem „unsichere Software" an der Wurzel gepackt. Am 08.10.2008 hat das Software Assurance Forum for Excellence in Code (kurz SAFECode) den Leitfaden Fundamental Practices for Secure Software Development veröffentlicht. Die Organisation, der u. a. Microsoft, EMC und SAP angehören, hat sich zum Ziel gesetzt, zur Verbesserung von Methoden der Softwareentwicklung beizutragen – mit dem besonderen Schwerpunkt Sicherheit.

Das 22-seitige Dokument fasst nach Einschätzung der Autoren die zur Zeit effektivsten Methoden zur sicheren Entwicklung von Software zusammen. Die Darstellung praxiserprobter Vorgehensweisen wird ergänzt durch Verweise auf weiterführende Informationen. Daher kann der Leitfaden gut als Einstieg in die sichere Softwareentwicklung genutzt

werden. Er ergänzt die Übersicht über Fallstudien zum Thema sichere Softwareentwicklung, Software Assurance: An Overview of Current Industry Best Practices, die im Februar 2008 von SAFECode publiziert wurde.

Mühsam nährt sich der Spammer

Nicht nur Stammzellenforschung bringt Ethikkonflikte mit sich – bisweilen auch die IT-Sicherheit: Dürfen Forscher Spam-Mails verschicken, um deren Erfolg oder Misserfolg zu bestimmen? Ein Team aus Berkeley und San Diego (UCSD) stellt in einem Konferenzbeitrag vom 28.10.2008 dar, wie es einen Teil eines Bot-Netzes „zurückkaperte", um die ohnehin darüber versandten Spam-Mails zur statistischen Auswertung zu markieren. Neben dem Wirkungsgrad verschiedener Spam-Filter zeigte sich: Nur knapp eine von zehn Millionen Mails führt zum Kauf der beworbenen blauen Pillen.

Wie die Forscher aus der Strichprobe hochrechnen, dürfte die Marge bei diesem Aufwand-Ertrags-Verhältnis so gering sein, dass weiter verbesserte Anti-Spam-Techniken das Geschäftsmodell empfindlich treffen könnten. Das gibt Hoffnung auf ein mögliches Ende der Plage.

Social Communities für Eltern

Am 04.09.2008 veröffentlichte die Medienkompetenz-Initiative Klicksafe, ein Projekt der Landeszentrale für Medien und Kommunikation Rheinland-Pfalz (LMK), der Landesanstalt für Medien Nordrhein-Westfalen (LfM) und des Europäischen Zentrums für Medienkompetenz (ecmc) eine Handreichung für Eltern zum Thema Social Communities.

Der Kurzratgeber erklärt auf 12 Seiten kompakt und gut verständlich, welche Risiken auf Kinder und Jugendliche bei der Nutzung von Communities wie SchülerVZ & Co. sowie in den beliebten Chatrooms lauern. Die wichtigsten Punkte, die man mit seinen Kindern besprechen sollte, werden erläutert und durch Links auf weiterführende Informationen und Kontaktadressen ergänzt.

Unserer Ansicht nach eine empfehlenswerte Lektüre und ein gutes Hilfsmittel für Eltern – im übrigen nicht das einzige, das sich in der umfangreichen Materialsammlung der Initiative findet.

Neuer NIST-Signaturstandard

Das US-amerikanische National Institute of Standards and Technology (NIST) hat am 12.11.2008 die Entwurfsfassung eines neuen Standards für Digitale Signaturen (FIPS-186-3) veröffentlicht. Der Nachfolger des angejährten FIPS 186-2 vom Januar 2000 unterscheidet sich schon im Umfang erheblich: Aus 76 Seiten wurden 125, allein der „Kern" des Standards (ohne Anhänge) wuchs von vier auf 19 Seiten. Neben den auf dem Diskreten Logarithmusproblem basierenden Signaturverfahren DSA und ECDSA sind nun auch RSA-Signaturen Teil des Standards – nicht mehr nur als kurzer Verweis auf ANSI X.9.31, sondern mit einer mehrseitigen Darstellung der Anforderungen z. B. an die Schlüsselgenerierung. Deutlich erweitert wurden die Anhänge zur Primzahl- und Parameterberechnung.

Die Neufassung des Standards geht deutlich über den eigentlichen Zweck hinaus: Er wurde zu einem ausgewachsenen Leitfaden für Einsteiger und Programmierer erweitert. Der Qualität zukünftiger Implementierungen könnte das zuträglich sein.

Secorvo News

Secorvo College aktuell

Für die rechtzeitige Planung der Weiterbildung 2009 lohnt ein Blick in den Seminarkalender 2009. Neben vier Terminen zum Abschluss der TISP-Zertifizierung bietet Secorvo College 2009 erstmals – im Februar und im Oktober – die Zertifizierung zum CPSSE an: dem Certified Professional for Secure Software Engineering. Das Zertifikat wurde von ISSECO, dem International Secure Software Engineering Council, unter Beteiligung von u. a. der SAP AG entwickelt.

Detaillierte Seminarprogramme und die Möglichkeit zur Online-Anmeldung finden Sie unter http://www.secorvo.de/college.

Über Originale und Fälschungen

Mit Dongles fing alles an – zwanzig Jahre später spricht man vom „Digital Rights Management", wenn es um den Schutz digitaler Güter geht. War es zunächst nur Software, die vor lizenzwidriger Verbreitung geschützt werden musste, zählen heute auch Daten zu den Schutzgütern – Musikaufnahmen, (Hör-) Bücher, Filme.

Auf dem letzten diesjährigen Event der Karlsruher IT-Sicherheitsinitiative (KA-IT-Si) wird Rüdiger Kügler von Wibu Systems, einem der Pioniere auf diesem Gebiet, am 04.12.2008 (Schlosshotel Karlsruhe, Beginn: 18 Uhr) spannende Rück-, Ein- und Ausblicke in die rasante Entwicklung des Lizenzmanagements geben. Im Anschluss gibt es wie gewohnt Gelegenheit zum „Buffet-Networking". Um Anmeldung wird gebeten.

Veranstaltungshinweise

Auszug aus http://www.veranstaltungen-it-sicherheit.de

November 2008	
25.11.	OWASP Germany 2008 Conference (www.owasp.org, Frankfurt)
Dezember 2008	
02.-04.12.	Sichere Softwareentwicklung (Secorvo, Karlsruhe)
04.12.	Das Original ist die beste Kopie (KA-IT-Si, Karlsruhe)
27.-30.12.	25th Chaos Communication Congress (CCC, Berlin)
Januar 2009	
20.-22.01.	Omnicard 2009 (inTIME, Berlin)
Februar 2009	
03.-04.02.	19. SmartCard-Workshop (Fraunhofer, Darmstadt)
10.-12.02.	Certified Professional for Secure Software Engineering (CPSSE) (Secorvo College, Karlsruhe)
22.-25.02.	16th Int. Workshop on Fast Software Encryption (IACR, Leuven/BE)
23.-26.02.	13th Financial Cryptography and Data Security 2009 (Int. Financial Cryptography Association, Barbados)

Fundsache

Der lesenswerte Leitfaden zur Nutzung von E-Mail und Internet im Unternehmen des BITKOM erschien im Januar 2008 in der aktualisierten Version 1.5. Das Dokument gibt einen Überblick über die Rechtslage, leitet daraus Empfehlungen für die rechtskonforme Gestaltung der E-Mail- und Internetnutzung ab und schließt mit Formulierungsvorschlägen für eine Betriebsvereinbarung.

Impressum

http://www.secorvo-security-news.de

ISSN 1613-4311

Redaktion: Dirk Fox, Stefan Gora, Kai Jendrian, Hans-Joachim Knobloch

Herausgeber (V. i. S. d. P.): Dirk Fox
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses:
security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an
redaktion-security-news@secorvo.de

secorvo
security consulting

Secorvo Security News

Dezember 2008

Editorial: Pyrrhussiege

Einige zehntausend Kreditkartennummern der Landesbank Berlin auf Microfiche, vom Kurier gegen einen Christstollen getauscht. Bankverbindungen von 21 Mio. Bundesbürgern auf dem Schwarzmarkt, für kleines Geld von Call-Center-Mitarbeitern eingesammelt. CD mit 17 Mio. Kundendaten von T-Mobile aufgetaucht, von einem Dienstleister mit umfangreichen Berechtigungen entwendet. Alles Variationen desselben Themas: Zunehmend vertrauen Unternehmen sensible Unternehmens- und Personendaten Dritten an – die das Vertrauen nicht immer verdienen.

Zwar sind die Motive für eine Auslagerung von Tätigkeiten an externe Dienstleister ebenso berechtigt wie nachvollziehbar. Für größere Flexibilität und transparentere Kosten zahlt man aber einen versteckten Preis: geringere Loyalität und Bindung an das beauftragende Unternehmen, eingeschränkter Einfluss auf die Prozesse und geringes Verständnis der Kerngeschäftsprozesse beim Dienstleister.

Für zahlreiche Tätigkeiten mag das unproblematisch sein. Immer öfter aber sind sensible Daten betroffen, die eine hohe Zuverlässigkeit und Vertrauenswürdigkeit des Personals erfordern: Reinigungskräfte, die sich außerhalb der regulären Arbeitszeiten im Unternehmen bewegen; Kuriere, die vertrauliche Daten unverschlüsselt transportieren; IT-Dienstleister, die Zugriff auf unternehmenskritische Daten erhalten.

Unabhängig von der erforderlichen Basis-Qualifikation, die für eine Dienstleistung erforderlich ist, erfordert ein angemessener Umgang mit sensiblen Daten jedoch sowohl hohe Loyalität und Vertrauenswürdigkeit als auch ein Mindestmaß an Verständnis für die Bedeutung der Daten, um Schäden durch Nachlässigkeit zu vermeiden.

So entpuppen sich die schönen Reduktionen auf der Ausgabenseite der Bilanz immer öfter als Pyrrhussieg. Denn externe Dienstleistung erfordert sorgfältige Auswahl und Kontrolle – wer das vernachlässigt, zahlt meist einen hohen Preis, wenn etwas schief geht.

Inhalt

secorvo
security consulting

Security News

Autorun deaktiviert?

Seit vielen Jahren predigen Security-Experten, wie gefährlich das automatische Starten von Anwendungen auf Wechseldatenträgern mittels Autorun-Funktionalität ist, haben Viren und Würmer so doch leichtes Spiel. Glücklicherweise ist das Deaktivieren der Autorun-Funktion in Windows technisch trivial und wird daher in vielen Unternehmen zentral über Group Policy Objekte durchgesetzt.

Aber ist es wirklich so trivial? Still und heimlich gestand Microsoft in einem Technet-Artikel vom 10.10.2008, dass das Setzen von NoDriveTypeAutorun in der Windows-Registry nicht ausreicht – und beschrieb die korrekte Erzwingung der Deaktivierung des Autorun-Registrierungsschlüssels in Windows. In vielen Umgebungen wird „die Autorun-Features nicht ordnungsgemäß deaktiviert", selbst wenn die Registry-Schlüssel korrekt gesetzt waren. Microsoft reagierte nun mit zahlreichen Updates sowie einem weiteren Registry-Schlüssel, genannt „HonorAutorunSetting". Nomen est omen. Peinlich, peinlich.

Handys aller Orten

Die Positionsbestimmung von Mobiltelefonen durch eifersüchtige Ehepartner und andere Bedarfsträger ist schon seit einer Weile einer der gefragtesten Location Based Serivices (LBS) für Mobilfunknetze. Zwar lassen sich LBS am Handy deaktivieren; dazu haben die deutschen Provider am 14.10.2008 eine Selbstverpflichtung auf ein einheitliches Verfahren veröffentlicht. Aber auch wenn auf dem Handy keine LBS aktiviert sind, werden Bewegungsdaten an Dritte weiter gegeben: So meldete T-Traffic am 03.11.2008, dass für die Stauprognose auf die Bewegungsdaten von 34 Millionen Handys im Netz der T-Mobile zugegriffen wird – „natürlich anonym". Pikant: T-Traffic wurde am 20.11.2008 von einer Nokia-Tochter in den USA übernommen; die Daten verlassen also den Geltungsbereich der EU-Datenschutzrichtlinie. Auch der Mitbewerb gibt sich nicht zugeknöpfter: Bereits am 14.01.2008 vereinbarte Vodafone Ähnliches mit TomTom.

Dass Handy-Ortung mit besseren Funkmessdaten noch präziser funktioniert als auf den Radius der mehr oder minder großen Funkzelle genau, gehört zur Lehrbuchweisheit. Am 01.12.2008 verkündete Bayerns Innenminister den praktischen Vollzug: Das dortige LKA hat in einer Art „Wardriving per Streifenwagen" einen Großteil der Mobilfunkzellen im Land vermessen und kartografiert. Eingesetzt wird das System zur Suche nach Verunglückten – und „noch nicht" zur Fahndung.

Alles in allem ein paar gute Gründe (mehr), das Handy immer öfter einfach abzuschalten.

Blackberry zertifiziert

Vor mehr als drei Jahren wurde nach einem umstrittenen Kurzgutachten des BSI das Testlabor des Fraunhofer Instituts SIT in Darmstadt vom Hersteller Research in Motion (RIM) mit einer Analyse der Sicherheit des Blackberry-Dienstes beauftragt. Am 24.11.2008 wurden nun das lange erwartete Zertifikat (gültig für BES v4.1.6) und der 33seitige Zertifizierungsbericht veröffentlicht.

Das Ergebnis ist eindeutig und belegt die Sorgfaltsmängel des BSI-Gutachtens vom Herbst 2005: „In our analysis of the BlackBerry Enterprise Solution, we did not find any evidence for the existence of a master key, back door or a function that would allow RIM to read customer's emails." Es ergänzt die von Secorvo im November 2005 publizierte Analyse der Blackberry-Architektur um eine Bestätigung der korrekten Implementierung des AES-256 und des Schlüsselmanagements.

Neben den im Zertifizierungsbericht enthaltenen Hinweisen zur sicheren Konfiguration des BES ist der „Blackberry Hardening Guide" des australischen Department of Defense vom 18.12.2007 zu empfehlen. Er enthält auf 27 Seiten zahlreiche detaillierte Konfigurationstipps für die sichere Nutzung des Blackberry – einschließlich Vorgaben für die Nutzung von S/MIME, PGP und TLS.

ePA-Akteptanzstellen gesucht

Es hat etwas von einem Gewinnspiel: Aus Unternehmen, Institutionen und Behörden, die bis zum 28.02.2009 dem Aufruf zum Anwendungstest für den elektronischen Personalausweis (ePA) – nicht zu verwechseln mit EPa – folgen, werden zehn ausgewählt. Sie können schon ab 01.10.2009 mit fachlicher Unterstützung des Bundesministeriums des Innern (BMI) die Nutzung des Identitätsnachweises über den ePA im Internet, an Automaten oder anderen Akzeptanzstellen erproben.

Leichtfertig sollte man dem Aufruf vom IT-Gipfel in Darmstadt am 20.11.2008 jedoch nicht mit seiner Registrierung folgen. Denn auch dieses Gewinnspiel hat einen Haken: Alle Bewerber – auch die nicht ausgewählten, deren Testphase nach Zeitplan am 01.12. 2009 beginnt – verpflichten sich, zahlreiche Eigenleistungen zu erbringen, von der Beschaffung bisher noch nicht verfügbarer Komponenten über die Akquise von Probanden bis zu gemeinsamen Marketing-Aktionen mit dem BMI. Bei positivem Testverlauf müssen sie ab dem Stichtag der ePA-Ausgabe am 01.11.2010 den ePA-Identitätsnach-

weis auch produktiv allen Ausweisinhabern unter ihren Nutzern anbieten.

Forensische Päckchen

Helix hat es vorgemacht (vgl. SSN 10/2008) – nun haben zwei weitere Anbieter neue Versionen ihrer kostenlosen forensischen Live-CDs veröffentlicht.

DEFT Linux (Digital Evidence & Forensic Toolkit) erschien am 28.11.2008 bereits in Version 4.01. Die Unterschiede zu Helix sind allerdings marginal: neben zu erwartenden Tools wie Autopsy, Sleuthkit oder foremost umfasst DEFT Linux Tools für Penetrationstests, bspw. Nessus und nmap. Vorsicht ist jedoch beim Anschluss externer Analyseplatten geboten: entgegen forensischer Best Practice werden diese nicht „read only“ eingebunden.

Äußerst vielversprechend sieht Version 0.4 von CAINE (Computer Aided INvestigative Environment) aus, die am 05.12.2008 veröffentlicht wurde. Auch CAINE bringt Standard-Tools mit, beinhaltet aber auch unbekanntere Forensiktools wie guymager, SFDumper oder Fundl. Herausragend ist das für Forensiker so wichtige Erstellen von Reports: CAINE stellt Mechanismen zur Verfügung, den Output der unterschiedlichen Tools in einem einheitlichen Format zu integrieren und erleichtert damit den Analyseprozess erheblich.

OWASP-Start in Deutschland

Über 100 Teilnehmer konnten sich am 25.11.2008 in Frankfurt davon überzeugen, dass das Thema Web Application Security inzwischen auch in Deutschland angekommen ist. Trotz äußerst kurzer Vorlaufzeit war die erste OWASP-Konferenz OWASP Germany 2008 sowohl im Hinblick auf die inhaltliche Qualität als auch auf die Teilnehmerzahl ein voller Erfolg. Es wurden technische Themen wie z. B. "Server- und Browser-basierte XSS Erkennung" oder "SOA Sicherheitsarchitektur" und nicht-technische Themen wie z. B. "Wirtschaftlichkeitsbetrachtungen von IT-Sicherheitsmaßnahmen" behandelt. Den Besuchern früherer KA-IT-Si-Veranstaltungen wird der Vortrag "Goldene Regeln der IT-Sicherheit bei der Beauftragung und Erstellung von Software" bekannt vorgekommen sein. Auch diese Konferenz bestätigt, dass sich die OWASP-Organisation national und international zu einer festen Größe im Zusammenhang mit der Sicherheit von (Web-)Applikationen entwickelt hat. Allen, die die Konferenz nicht besuchen konnten oder die Vorträge noch einmal nachvollziehen möchten, stehen die Präsentationsfolien auf der Konferenzseite zur Verfügung.

Flickwerk Patchen

Dass das Aktualisieren von Systemen und Anwendungen inzwischen eine herausfordernde und aufwändige Aufgabe darstellt, ist nichts Neues. Lücken im Patch-Management finden sich daher nicht selten – und sollten zügig geschlossen werden. Das unterstreicht eine aktuelle Veröffentlichung des Anbieters Secunia, der am 25.11.2008 Version 1.0 des für den Privatgebrauch kostenlosen Personal Software Inspector veröffentlichte. Die Auswertung der Analyseergebnisse von über 20.000 (überwiegend privaten) Client-Systemen nach einer Woche zeigte, dass weniger als 2 % der Systeme sowohl beim Betriebssystem als auch bei weiteren installierten Programmen auf einem aktuellen Stand waren.

Angesichts der Zunahme aufgedeckter sicherheitskritischer Bugs und immer kürzerer Reaktionszeiten der Angreifer-Szene ist eine regelmäßige Analyse des Patch-Stands sehr zu empfehlen.

Secorvo News

Secorvo College aktuell

Für Ihr großes Interesse am Weiterbildungsangebot von Secorvo College im Jahr 2008 danken wir Ihnen. Die starke Nachfrage und die vielen positiven Rückmeldungen haben uns sehr gefreut. Wir hoffen, Sie im kommenden Jahr auf einer unserer Veranstaltungen wiederzusehen – einen aktuellen Überblick finden Sie in unserem Seminarkalender 2009.

Auch für Ihre Anregungen und Themenwünsche an college@secorvo.de sind wir dankbar. Detaillierte Seminarprogramme und die Möglichkeit zur Online-Anmeldung finden Sie unter http://www.secorvo.de/college.

Zum Schluss …

Hinter uns liegen 10 Jahre aktiver Mitwirkung an IT-Sicherheit und Datenschutz in Deutschland – und das erfolgreichste Jahr unserer Firmengeschichte. Wir danken Ihnen für Ihr Vertrauen und freuen uns auf viele weitere herausfordernde und spannende Jahre der Zusammenarbeit.

Wir wünschen Ihnen besinnliche Feiertage – und für 2009 neue Ideen, Visionen und gutes Gelingen!

Veranstaltungshinweise

Auszug aus http://www.veranstaltungen-it-sicherheit.de

Dezember 2008	
27.-30.12.	25th Chaos Communication Congress (CCC, Berlin)
Januar 2009	
20.-22.01.	Omnicard 2009 (inTIME, Berlin)
Februar 2009	
03.-04.02.	19. SmartCard-Workshop (Fraunhofer, Darmstadt)
10.-12.02.	Certified Professional for Secure Software Engineering (CPSSE) (Secorvo College, Karlsruhe)
19.02.	Bingo-Voting - verifizierbare elektronische Wahlen (KA-IT-Si, Karlsruhe)
22.-25.02.	16th Int. Workshop on Fast Software Encryption (IACR, Leuven/BE)
März 2009	
09.-13.03.	T.I.S.P.-Schulung (Secorvo College)
17.-18.03.	16. DFN Workshop - Sicherheit in vernetzten Systemen (DFN-CERT, Hamburg)
17.-19.03.	IT-Sicherheitsaudits (Secorvo College)

Fundsache

Microsoft hat am 10.11.2008 eine öffentliche Beta-Version des "SDL Threat Modelling Tool v3.1" zum Download bereitgestellt. Die Bedrohungsanalyse (Threat Modelling) spielt im Secure Development Lifecycle (SDL) eine wichtige Rolle. Erste Tests mit diesem Tool hinterließen einen positiven Eindruck. Das Threat Modelling Tool findet sich u. a. im Tools Repository zum SDL.

Impressum

http://www.secorvo-security-news.de

ISSN 1613-4311

Redaktion: Dirk Fox, Stefan Gora, Kai Jendrian, Stefan Kelm, Hans-Joachim Knobloch

Herausgeber (V. i. S. d. P.): Dirk Fox
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses:
security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an
redaktion-security-news@secorvo.de